VORLESUNGEN

ÜBER

ZAHLENTHEORIE

VON

P. G. LEJEUNE DIRICHLET.

HERAUSGEGEBEN

UND

MIT ZUSÄTZEN VERSEHEN

VON

R. DEDEKIND,

Professor der höheren Mathematik am Collegium Carolinum zu Braunschweig.

ZWEITE

UMGEARBEITETE UND VERMEHRTE AUFLAGE.

ZWEITE ABTHEILUNG.

BRAUNSCHWEIG,

DRUCK UND VERLAG VON FRIEDRICH VIEWEG UND SOHN.

1871.

ANKÜNDIGUNG.

Die Vorlesungen über Zahlentheorie, welche von Dirichlet in Berlin und später in Göttingen gehalten sind, haben einen so bedeutenden Erfolg gehabt, dass schon öfter der Wunsch nach einer möglichst getreuen Publication derselben ausgesprochen worden ist. Da in frühern Zeiten die Zahlentheorie weder auf Schulen noch auf Universitäten Gegenstand des Unterrichts war, und da es auch an eigentlichen Lehrbüchern für diesen Theil der Mathematik fehlte, so mussten diese Vorlesungen mit den ersten Elementen, mit der Lehre von der Theilbarkeit der Zahlen beginnen; andererseits erstreckten sie sich bis zu den feinen von Dirichlet in die Wissenschaft eingeführten Methoden, welche in der Anwendung der Infinitesimal-Rechnung auf Probleme der Zahlentheorie bestehen. Bei der jetzigen Herausgabe ist dieser Umfang beibehalten, um den Studirenden ein Lehrbuch in die Hand zu geben, welches nicht blos die unentbehrlichen Grundlagen für jedes Studium der Zahlentheorie, sondern auch die neuen Principien enthält, durch welche dieselbe in die innigste Verbindung mit anderen Theilen der Mathematik getreten ist.

Mit der hiermit erfolgenden zweiten Abtheilung ist das Werk in der neuen Auflage beendigt.

VORWORT DES HERAUSGEBERS.

Gleich nach dem Tode *Dirichlet's* wurde ich mehrfach aufgefordert, die von ihm gehaltenen Universitäts-Vorlesungen, welche so ausserordentlich viel zur Verbreitung der Bekanntschaft mit neueren und feineren Theilen der Mathematik beigetragen haben, in möglichst getreuer Form zu veröffentlichen; ich glaubte dieser Aufforderung um so eher nachkommen zu können, als ich in den Jahren 1855 bis 1858 die wichtigsten dieser Vorlesungen in Göttingen gehört und ausserdem vielfach Gelegenheit gehabt hatte, im persönlichen Verkehr *Dirichlet's* Gründe für die von ihm befolgte Methode des Vortrags kennen zu lernen. Nachdem auch die Verwandten *Dirichlet's* mich dazu ermächtigt haben, so übergebe ich dem mathematischen Publicum hiermit eine Ausarbeitung der Vorlesung über Zahlentheorie, bei welcher im Wesentlichen der im Winter 1856 bis 1857 von *Dirichlet* befolgte Gang eingehalten ist; er selbst fasste damals den Gedanken einer Herausgabe dieser Vorlesungen, und da er seinen

Vortrag nie schriftlich ausgearbeitet hatte, so diente ihm ein von mir geschriebenes, allerdings nur die Hauptmomente der Beweise enthaltendes Heft dazu, einen ungefähren Ueberschlag über die Ausdehnung der einzelnen Abschnitte zu machen. In öfter wiederkehrenden Gesprächen über diesen Plan äusserte er die Absicht, bei der Veröffentlichung manche Abschnitte hinzufügen zu wollen, die in einem Lehrbuch nicht fehlen dürften, die aber in jener Wintervorlesung aus Mangel an Zeit übergangen werden mussten. Bei der jetzigen Herausgabe ist daher im Wesentlichen zwar das eben erwähnte Heft zu Grunde gelegt, aber ich habe theils nach älteren Heften, theils nach *Dirichlet'schen* Abhandlungen, endlich auch ganz nach eigenem Ermessen Zusätze von nicht unbedeutender Ausdehnung gemacht, welche ich hier anführen zu müssen glaube, um für sie die Verantwortlichkeit zu übernehmen; sie sind in den Paragraphen 105 bis 110, 121 bis 144 und in den unmittelbar unter den Text gesetzten Anmerkungen enthalten.

Es ist meine Absicht, diesem ersten Bande, dessen Vollendung durch andere Arbeiten sich bis jetzt verzögert hat, zunächst einen zweiten weniger umfangreichen nachfolgen zu lassen, in welchem die Vorlesung über die im umgekehrten Verhältniss des Quadrats der Entfernung wirkenden Kräfte wiedergegeben werden soll.

Braunschweig, im October 1863.

R. Dedekind.

VORWORT ZUR ZWEITEN AUFLAGE.

Diese neue Auflage unterscheidet sich von der ersten hauptsächlich dadurch, dass sie um das zehnte Supplement bereichert ist, welches von der Composition der Formen handelt. Dieser Gegenstand war bei der ersten Auflage gänzlich ausgeschlossen geblieben, weil die einzige Abhandlung *Dirichlet's*, welche sich unmittelbar hierauf bezieht, nur den ersten Fundamentalsatz behandelt, weshalb ich befürchten musste, bei einer vollständigen Darstellung dieser Theorie mich zu weit von dem ursprünglichen Zwecke der Herausgabe zu entfernen. Obwohl ich nun diese Gefahr auch jetzt durchaus nicht verkenne, so habe ich mich doch aus vielen Gründen entschlossen, das zehnte Supplement hinzuzufügen und dadurch mehrfachen an mich gerichteten Aufforderungen nach besten Kräften zu entsprechen, hauptsächlich, weil trotz des ungemeinen Interesses und der steigenden Wichtigkeit dieser Theorie noch immer kein Versuch gemacht ist, die grossen Schwierigkeiten hinwegzuräumen, welche beim Eindringen

in dieselbe sich dem Anfänger entgegenstellen, und weil die übrigen Abschnitte des Werkes ganz vorzüglich geeignet sind, einen solchen Versuch zu erleichtern. Bei der wirklichen Ausführung dieses Entschlusses habe ich mich nicht auf die Begründung der ersten Elemente beschränkt, sondern es für nothwendig gehalten, den grössten Theil der in der fünften Section der *Disquisitiones Arithmeticae* enthaltenen Untersuchungen möglichst kurz und einfach zur Darstellung zu bringen. Endlich habe ich in dieses Supplement eine allgemeine Theorie der *Ideale* aufgenommen, um auf den Hauptgegenstand des ganzen Buches von einem höheren Standpuncte aus ein neues Licht zu werfen; hierbei habe ich mich freilich auf die Darstellung der Grundlagen beschränken müssen, doch hoffe ich, dass das Streben nach charakteristischen Grundbegriffen, welches in anderen Theilen der Mathematik mit so schönen Erfolgen gekrönt ist, mir nicht ganz missglückt sein möge. Die Untersuchungen in diesem von *Kummer* geschaffenen Gebiete, welche *Kronecker* vor vierzehn Jahren angestellt hat, sind bis jetzt nicht veröffentlicht, und ich vermag nach den damaligen brieflichen Mittheilungen dieses ausgezeichneten Mathematikers nicht zu beurtheilen, in welchen Beziehungen seine Principien zu den meinigen stehen. Der Aufbau der Theorie in §. 163 befriedigt mich selbst zwar noch nicht vollständig; allein es ist mir erst nach sehr langem Nachdenken geglückt, ihm diese Form zu geben, während ich vor etwa zehn Jahren von der Theorie der höheren Congruenzen in Verbindung mit den Principien von *Galois* zu einer ganz anderen Begründungsart gelangt war, welche einige

Berührungspuncte mit der Theorie der idealen Zahlen von *Selling* hat, mir aber jetzt weniger naturgemäss erscheint. Eine ausführlichere Darstellung der an den Begriff eines *Körpers* (§. 159) sich anschliessenden algebraischen Principien, welche hier nur beiläufig angedeutet werden konnten, verspare ich mir für eine andere Gelegenheit.

Es ist natürlich, dass die Hinzufügung des zehnten Supplementes einige Rückwirkung auf die früheren Abschnitte ausgeübt hat; doch braucht man nicht zu besorgen, dass ich mich durch solche Abänderungen der ersten Auflage im Plan und in der Haltung der Darstellung von der eigentlichen Grundlage, den Vorlesungen *Dirichlet's*, weiter entfernt habe. Um einem etwaigen Vorwurfe dieser Art von vornherein zu begegnen, wiederhole ich hier (aus den Göttinger Gelehrten Anzeigen vom 27. Januar 1864), dass auch die erste Auflage sich nicht auf ein in den Vorlesungen selbst nachgeschriebenes Heft, sondern nur auf Notizen stützt, welche ich aus der Erinnerung und grösstentheils in äusserst kurzer Form verfasst habe; als ich diese Vorlesungen als Privatdocent in Göttingen hörte, war ich mit dem Stoffe hinreichend vertraut, und mein Hauptzweck bestand darin, den überaus eindringlichen Vortrag *Dirichlet's* vollständig auf mich wirken zu lassen. Bei der Herausgabe der ersten Auflage, welche erst nach einer Reihe von Jahren erfolgte, wurde es nothwendig, diese Notizen ganz neu auszuarbeiten und auch durch eigene Zuthaten (z. B. §. 2, wenn ich nicht irre) zu ergänzen, die unmöglich alle erwähnt werden konnten. Aber damals sowohl wie jetzt

ist es mein eifrigstes Streben gewesen, *Dirichlet's* Vortrag mit grösster Treue wiederzugeben. Volle Freiheit habe ich mir dagegen bei den eigenen Zusätzen gestattet; gänzlich umgearbeitet sind z. B. die §§. 105 bis 110, 143, 144, und manches Neue ist theils im Text, theils in Form von Noten hinzugefügt.

Endlich habe ich mich bemüht, überall, wo es mir möglich war, auf die Quellen zu verweisen, um den Leser zum Studium der Originalwerke zu veranlassen und in ihm ein Bild von den Fortschritten der Wissenschaft zu erwecken, deren ebenso tiefe wie erhabene Wahrheiten einen Schatz bilden, welcher die unvergängliche Frucht eines wahrhaft edelen Wettkampfes der europäischen Völker ist.

Braunschweig, 1. März 1871.

R. Dedekind.

INHALT.

Seite

Zweiter Abschnitt: Von der Congruenz der Zahlen.

Dritter Abschnitt: Von den quadratischen Resten.

Vierter Abschnitt: Von den quadratischen Formen.

Supplemente.

§. 113.

Wir wollen jetzt Summen betrachten, welche die vorstehende als speciellen Fall enthalten; wir bezeichnen mit n irgend eine ganze positive Zahl, mit h irgend eine positive oder negative ganze Zahl, und setzen zur Abkürzung

$$\Sigma\, e^{s^2\frac{2h\pi i}{n}} = \varphi(h, n),$$

wo der Summationsbuchstabe s irgend ein vollständiges Restsystem in Bezug auf den Modulus n durchlaufen muss. Mit Hülfe dieser Bezeichnungsweise können wir den im vorigen Paragraphen bewiesenen Satz in folgender Weise ausdrücken:

$$\varphi(1, n) = (1+i)\sqrt{n}, \quad \text{wenn} \quad n \equiv 0 \pmod 4.$$

Der Ausdruck $\varphi(h,n)$ besitzt nun die folgenden drei Eigenschaften:

1. Ist $h \equiv h' \pmod n$, so ist

$$\varphi(h, n) = \varphi(h', n);$$

dies folgt unmittelbar daraus, dass für jeden ganzzahligen Werth von s stets

$$e^{s^2\frac{2h\pi i}{n}} = e^{s^2\frac{2h'\pi i}{n}}$$

ist.

2. Ist a relative Primzahl gegen n, so ist

$$\varphi(ha^2, n) = \varphi(h, n);$$

denn es ist

$$\varphi(ha^2, n) = \Sigma\, e^{(as)^2\frac{2h\pi i}{n}},$$

und wenn s ein vollständiges Restsystem nach dem Modul n durchläuft, so gilt (nach §. 18) dasselbe von as.

3. Sind m, n irgend zwei relative Primzahlen, und beide positiv, so ist

$$\varphi(hm, n)\,\varphi(hn, m) = \varphi(h, mn).$$

Es ist nämlich

$$\varphi(hm, n) = \Sigma\, e^{s^2 \frac{2hm\pi i}{n}}, \quad \varphi(hn, m) = \Sigma\, e^{t^2 \frac{2hn\pi i}{m}},$$

wo die Buchstaben s, t vollständige Restsysteme resp. in Bezug auf die Moduln n, m durchlaufen müssen; und folglich ist

$$\varphi(hm, n)\ \varphi(hn, m) = \Sigma\, e^{\left(\frac{ms^2}{n} + \frac{nt^2}{m}\right) 2h\pi i},$$

wo das Summenzeichen rechter Hand sich auf alle mn Combinationen jedes Werthes von s mit jedem Werthe von t bezieht. Da nun

$$\frac{ms^2}{n} + \frac{nt^2}{m} = \frac{(ms + nt)^2}{mn} - 2st$$

ist, und alle Multipla von $2\pi i$ im Exponenten fortgelassen werden können, so ist auch

$$\varphi(hm, n)\ \varphi(hn, m) = \Sigma\, e^{(ms+nt)^2 \frac{2h\pi i}{mn}},$$

wo das Summenzeichen sich wieder auf sämmtliche Werthe von s und t bezieht. Setzt man nun

$$ms + nt = r,$$

so nimmt r, wenn s und t alle ihnen zukommenden Werthe durchlaufen, im Ganzen mn Werthe an, und zwar sind diese alle incongruent nach dem Modulus mn; denn aus

$$ms + nt \equiv ms' + nt' \pmod{mn}$$

folgt

$$ms \equiv ms' \pmod{n}, \quad nt \equiv nt' \pmod{m}$$

und folglich, da m und n relative Primzahlen sind,

$$s \equiv s' \pmod{n}, \quad t \equiv t' \pmod{m};$$

d. h. die Zahl r nimmt nur dann Werthe an, welche nach dem Modul mn congruent sind, wenn die Werthe von s congruent nach dem Modul n, und gleichzeitig die Werthe von t congruent nach dem Modul m sind. Den mn verschiedenen Combinationen von s und t correspondiren daher mn Werthe von r, welche nach dem Modul mn incongruent sind, und folglich bilden diese Werthe von r ein vollständiges Restsystem nach dem Modul mn. Es ist folglich

$$\varphi(hm, n)\ \varphi(hn, m) = \Sigma\, e^{r^2 \frac{2h\pi i}{mn}} = \varphi(h, mn),$$

was zu beweisen war.

§. 114.

Mit Hülfe dieser Sätze können wir nun den Werth von $\varphi(1,n)$, welcher für den Fall, dass $n \equiv 0 \pmod 4$ ist, schon in §. 112 gefunden ist, auch für alle andern Werthe der Zahl n bestimmen. Ist zunächst n irgend eine *ungerade* Zahl, so nehmen wir in dem letzten Satz des vorigen Paragraphen

$$h = 1, \quad m = 4,$$

und erhalten

$$\varphi(4, n)\, \varphi(n, 4) = \varphi(1, 4n);$$

nun ist nach dem zweiten Satze des vorigen Paragraphen

$$\varphi(4, n) = \varphi(2^2, n) = \varphi(1, n);$$

ferner ist

$$\varphi(n, 4) = 2(1 + i^n),$$

und nach dem in §. 112 gefundenen Resultat

$$\varphi(1, 4n) = (1 + i)\sqrt{4n} = 2(1 + i)\sqrt{n},$$

wo die Quadratwurzel $\sqrt{n}$ wieder positiv genommen werden muss. Hieraus ergiebt sich also

$$\varphi(1, n) \cdot 2(1 + i^n) = 2(1 + i)\sqrt{n}$$

oder

$$\varphi(1, n) = \frac{1 + i}{1 + i^n}\sqrt{n};$$

je nachdem nun $n \equiv 1$ oder $\equiv 3 \pmod 4$ ist, wird

$$i^n = i \quad \text{oder} \quad = -i$$

und folglich

$$\frac{1 + i}{1 + i^n} = 1 \quad \text{oder} \quad = \frac{1 + i}{1 - i} = i,$$

also

$$\varphi(1, n) = \sqrt{n} \quad \text{oder} \quad = i\sqrt{n};$$

diese beiden Fälle lassen sich aber in die eine Formel

$$\varphi(1, n) = i^{\frac{1}{4}(n-1)^2}\sqrt{n}$$

zusammenfassen.

Ist endlich n durch 2, aber nicht durch 4 theilbar, also das Doppelte einer ungeraden Zahl, so setzen wir in dem dritten Satze des vorigen Paragraphen $h = 1$, ferner $m = 2$, und $\frac{1}{2}n$ statt n, wodurch allen Bedingungen desselben Genüge geschieht, und erhalten

$$\varphi(2, \tfrac{1}{2}n)\ \varphi(\tfrac{1}{2}n, 2) = \varphi(1, n);$$

nun ist aber

$$\varphi(\tfrac{1}{2}n, 2) = 0,$$

und folglich auch

$$\varphi(1, n) = 0.$$

Wir wollen die so gewonnenen Resultate in folgender Tabelle zusammenfassen:

$$\begin{aligned} \varphi(1, n) &= (1+i)\sqrt{n}, && \text{wenn} \quad n \equiv 0 \pmod 4 \\ \varphi(1, n) &= i^{\frac{1}{4}(n-1)^2}\sqrt{n}, && \text{wenn} \quad n \equiv 1 \pmod 2 \\ \varphi(1, n) &= 0, && \text{wenn} \quad n \equiv 2 \pmod 4. \end{aligned}$$

Von der grössten Wichtigkeit ist aber die Bemerkung, dass die in den beiden ersten Formeln vorkommende Quadratwurzel $\sqrt{n}$ durchaus *positiv* genommen werden muss, wie es sich bei der Untersuchung in §. 112 herausgestellt hat. Ohne diese nähere Bestimmung würden die vorstehenden Sätze sich auf viel einfachere Art beweisen lassen; *Gauss* wurde zuerst in seiner Theorie der Kreistheilung auf die Betrachtung solcher Summen geführt*); es ergiebt sich dort ohne Schwierigkeit der Werth des Quadrates derselben; der viel tiefer liegenden Bestimmung des Vorzeichens der Quadratwurzel widmete er aber eine besondere Abhandlung**), in welcher er auf einem, von dem hier (in §. 112) eingeschlagenen gänzlich verschiedenen Wege, nämlich durch rein algebraische Zerlegung dieser Summen in Producte, vollständig zum Ziele gelangte.

---

*) *D. A.* art. 356.

**) *Summatio quarumdam serierum singularium.* 1808.

§. 115.

Wir suchen nun den Werth von $\varphi(h, n)$ auch für beliebige Werthe von h zu bestimmen, beschränken uns dabei aber auf den Fall, dass n eine ungerade Primzahl ist, die wir mit p bezeichnen wollen. Bezeichnen wir mit α die sämmtlichen $\frac{1}{2}(p-1)$ incongruenten quadratischen Reste von p, mit β die $\frac{1}{2}(p-1)$ quadratischen Nichtreste, so ist (nach §. 33)

$$\varphi(h, p) = \Sigma e^{s^2 \frac{2h\pi i}{p}} = 1 + 2 \Sigma e^{\alpha \frac{2h\pi i}{p}};$$

da ferner

$$1 + \Sigma e^{\alpha \frac{2h\pi i}{p}} + \Sigma e^{\beta \frac{2h\pi i}{p}} = \Sigma e^{s \frac{2h\pi i}{p}} = 0$$

ist, sobald h nicht durch p theilbar ist, so können wir für diesen Fall mit Benutzung des Legendre'schen Symbols

$$\varphi(h, p) = \Sigma e^{\alpha \frac{2h\pi i}{p}} - \Sigma e^{\beta \frac{2h\pi i}{p}} = \Sigma \left(\frac{s}{p}\right) e^{s \frac{2h\pi i}{p}}$$

setzen, wo s die Werthe $1, 2 \ldots (p-1)$ durchläuft. Da ferner

$$\left(\frac{hs}{p}\right) = \left(\frac{h}{p}\right)\left(\frac{s}{p}\right), \quad \left(\frac{h}{p}\right)\left(\frac{h}{p}\right) = 1$$

ist, so wird

$$\varphi(h, p) = \left(\frac{h}{p}\right) \Sigma \left(\frac{hs}{p}\right) e^{hs \cdot \frac{2\pi i}{p}},$$

oder, da h nicht theilbar durch p ist, und folglich hs gleichzeitig mit s ein vollständiges Restsystem nach dem Modul p durchläuft (mit Ausschluss der Zahl $\equiv 0$),

$$\varphi(h, p) = \left(\frac{h}{p}\right) \Sigma \left(\frac{s}{p}\right) e^{s \frac{2\pi i}{p}};$$

für $h = 1$ ergiebt sich

$$\varphi(1, p) = \Sigma \left(\frac{s}{p}\right) e^{s \frac{2\pi i}{p}}$$

und folglich (nach §. 114)

$$\varphi(h, p) = \left(\frac{h}{p}\right) \varphi(1, p) = \left(\frac{h}{p}\right) i^{\left(\frac{p-1}{2}\right)^2} \sqrt{p},$$

wo die Quadratwurzel $\sqrt{p}$ wieder positiv zu nehmen ist. (Wenn h durch p theilbar ist, so ergiebt sich unmittelbar aus der Definition dieser Summen $\varphi(h, p) = p$.)

Aus dem vorstehenden Resultate in Verbindung mit dem dritten Satze des §. 113 lässt sich nun auf ganz einfache Weise das Reciprocitätsgesetz in der Theorie der quadratischen Reste (§. 42) für je zwei positive ungerade Primzahlen p und q ableiten. Es ist nämlich

$$\varphi(q, p) = \left(\frac{q}{p}\right) i^{\frac{1}{4}(p-1)^2} \sqrt{p},$$

und ebenso

$$\varphi(p, q) = \left(\frac{p}{q}\right) i^{\frac{1}{4}(q-1)^2} \sqrt{q},$$

und nach dem vorhergehenden Paragraphen

$$\varphi(1, pq) = i^{\frac{1}{4}(pq-1)^2} \sqrt{pq},$$

und zwar sind alle Quadratwurzeln *positiv* zu nehmen, woraus folgt, dass

$$\sqrt{pq} = \sqrt{p}\sqrt{q}$$

ist. Nach dem dritten Satze des §. 113 ist nun

$$\varphi(p, q)\, \varphi(q, p) = \varphi(1, pq),$$

folglich

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) i^{\frac{1}{4}(p-1)^2 + \frac{1}{4}(q-1)^2} \sqrt{p}\,\sqrt{q} = i^{\frac{1}{4}(pq-1)^2} \sqrt{pq},$$

und also

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = i^{\lambda},$$

wo zur Abkürzung λ für

$$\frac{(pq-1)^2-(p-1)^2-(q-1)^2}{4} = \frac{p-1}{2}\,\frac{q-1}{2}\left\{(p+1)(q+1)-2\right\}$$

gesetzt ist; da nun

$$(p+1)(q+1) - 2 \equiv 2 \pmod 4$$

ist, so erhalten wir

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = i^{\frac{1}{2}(p-1)(q-1)} = (-1)^{\frac{1}{2}(p-1)\cdot\frac{1}{2}(q-1)},$$

womit der Reciprocitätssatz von Neuem bewiesen ist. Dieser Beweis rührt ebenfalls von *Gauss* her*).

*) *Summatio quarumdam serierum singularium.* 1808.

Auf ganz ähnliche Art lassen sich die Sätze (§§. 40, 41) über die Zahlen -1 und 2 beweisen. Aus dem obigen Satze

$$\varphi(h, p) = \left(\frac{h}{p}\right) \varphi(1, p) = \left(\frac{h}{p}\right) i^{\frac{1}{4}(p-1)^2} \sqrt{p}$$

folgt nämlich

$$\varphi(-1, p) = \left(\frac{-1}{p}\right) i^{\frac{1}{4}(p-1)^2} \sqrt{p};$$

andererseits ist

$$\varphi(-1, p) = \Sigma\, e^{e^2 \frac{2\pi(-i)}{p}},$$

und hieraus folgt, dass $\varphi(-1, p)$ durch Vertauschung von i mit $-i$ aus $\varphi(1, p)$ hervorgeht, dass also

$$\varphi(-1, p) = (-i)^{\frac{1}{4}(p-1)^2} \sqrt{p}$$

ist; durch Vergleichung dieser beiden Ausdrücke, in denen $\sqrt{p}$ beide Male positiv zu nehmen ist, ergiebt sich aber

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{1}{4}(p-1)^2} = (-1)^{\frac{1}{2}(p-1)}.$$

Setzen wir ferner in dem dritten Satz des §. 113

$$h = 1, \quad m = 8, \quad n = p,$$

so erhalten wir

$$\varphi(8, p)\ \varphi(p, 8) = \varphi(1, 8p);$$

nun ist aber

$$\varphi(1, 8p) = (1 + i)\sqrt{8p} = 4\sqrt{p} \cdot e^{\frac{1}{4}\pi i},$$

ferner

$$\varphi(p, 8) = 4 e^{\frac{1}{4}p\pi i},$$

ferner (nach dem zweiten Satze des §. 113)

$$\varphi(8, p) = \varphi(2 \cdot 2^2, p) = \varphi(2, p),$$

d. h.

$$\varphi(8, p) = \left(\frac{2}{p}\right) \varphi(1, p) = \left(\frac{2}{p}\right) i^{\frac{1}{4}(p-1)^2} \sqrt{p};$$

setzen wir diese Werthe für $\varphi(8, p)$, $\varphi(p, 8)$ und $\varphi(1, 8p)$ in die vorangehende Gleichung ein, so erhalten wir

$$\left(\frac{2}{p}\right) i^{\frac{1}{4}(p-1)^2} \sqrt{p} \cdot 4 e^{\frac{1}{4}p\pi i} = 4\sqrt{p} \cdot e^{\frac{1}{4}\pi i},$$

und hieraus folgt leicht

$$\left(\frac{2}{p}\right) = (-1)^{\frac{1}{8}(p^2-1)}.$$

Auf diese Weise sind alle Hauptsätze der Theorie der quadratischen Reste von Neuem bewiesen.

§. 116.

Für den Fall, dass p eine ungerade Primzahl, und h irgend eine durch p nicht theilbare ganze Zahl ist, haben wir im vorigen Paragraphen folgende Gleichung erhalten

$$\Sigma \left(\frac{s}{p}\right) e^{s\frac{2h\pi i}{p}} = \left(\frac{h}{p}\right) \varphi(1, p),$$

welche, wenn man den für $\varphi(1, p)$ gefundenen Werth einsetzt, in die folgende übergeht:

$$\Sigma \left(\frac{s}{p}\right) e^{s\frac{2h\pi i}{p}} = \left(\frac{h}{p}\right) i^{\frac{1}{4}(p-1)^2} \sqrt{p}; \tag{1}$$

soll dieselbe auch für den vorher ausgeschlossenen Fall, in welchem $h \equiv 0 \pmod{p}$ ist, ihre Gültigkeit behalten, so müssen wir übereinkommen, immer

$$\left(\frac{h}{p}\right) = 0$$

zu setzen, wenn h durch p theilbar ist; denn die linke Seite der Gleichung wird

$$\Sigma \left(\frac{s}{p}\right) = 0,$$

weil die Anzahl der quadratischen Reste genau gleich ist der Anzahl der quadratischen Nichtreste. Nach dieser Erweiterung des von Legendre eingeführten Zeichens wird ferner, wenn man an der in §. 46 gegebenen Erklärung des Jacobi'schen Symbols festhält, stets

$$\left(\frac{m}{P}\right) = 0,$$

wenn m keine relative Primzahl zu P ist.

Die Gleichung (1) gilt jetzt allgemein für jede positive ungerade Primzahl p, wenn h irgend eine ganze Zahl bedeutet, und die Summation linker Hand darf auch auf die Zahlclasse $s \equiv 0 \pmod{p}$ ausgedehnt werden. Wir wollen nun zeigen, dass dieser Satz über ungerade positive Primzahlen p sich genau in derselben Fassung

auch auf jede positive ungerade zusammengesetzte Zahl P übertragen lässt, welche durch keine Quadratzahl (ausser 1) theilbar ist. Wir setzen also

$$P = pp'p'' \ldots$$

wo $p, p', p'' \ldots$ lauter positive ungerade und von einander verschiedene Primzahlen bedeuten, und führen der Bequemlichkeit halber folgende Bezeichnung ein:

$$\frac{P}{p} = Q, \quad \frac{P}{p'} = Q', \quad \frac{P}{p''} = Q'' \ldots$$

Schreiben wir nun für jede der Primzahlen $p, p', p'' \ldots$ die obige Gleichung (1) auf:

$$\begin{aligned}
\Sigma \left(\frac{s}{p}\right) e^{s\frac{2h\pi i}{p}} &= \left(\frac{h}{p}\right) i^{\frac{1}{4}(p-1)^2} \sqrt{p} \\
\Sigma \left(\frac{s'}{p'}\right) e^{s'\frac{2h\pi i}{p'}} &= \left(\frac{h}{p'}\right) i^{\frac{1}{4}(p'-1)^2} \sqrt{p'} \\
\Sigma \left(\frac{s''}{p''}\right) e^{s''\frac{2h\pi i}{p''}} &= \left(\frac{h}{p''}\right) i^{\frac{1}{4}(p''-1)^2} \sqrt{p''} \\
&\cdots\cdots\cdots\cdots
\end{aligned}$$

und setzen wir zur Abkürzung

$$sQ + s'Q' + s''Q'' + \cdots = m,$$

so ergiebt, da auch nach der neuen Erweiterung des Legendre'schen Symbols stets

$$\left(\frac{h}{p}\right)\left(\frac{h}{p'}\right)\left(\frac{h}{p''}\right)\cdots = \left(\frac{h}{P}\right)$$

ist, die Multiplication aller dieser Gleichungen folgendes Resultat

$$\begin{aligned}
&\Sigma \left(\frac{s}{p}\right)\left(\frac{s'}{p'}\right)\left(\frac{s''}{p''}\right)\ldots e^{m\frac{2h\pi i}{P}} \\
&= \left(\frac{h}{p}\right) i^{\frac{1}{4}(p-1)^2 + \frac{1}{4}(p'-1)^2 + \frac{1}{4}(p''-1)^2 + \cdots} \sqrt{P},
\end{aligned} \tag{2}$$

wo $\sqrt{P}$ wieder positiv zu nehmen ist, und das Summenzeichen linker Hand sich auf alle $pp'p'' \ldots = P$ Combinationen aller Werthe von $s, s', s'' \ldots$ bezieht. Zunächst leuchtet nun ein, dass je zwei verschiedenen dieser Combinationen auch zwei nach dem Modulus P incongruente Werthe von m entsprechen; denn aus

$$sQ + s'Q' + s''Q'' + \cdots \equiv tQ + t'Q' + t''Q'' + \cdots \pmod{P}$$

würde, da Q', Q'' ... sämmtlich $\equiv 0 \pmod{p}$ sind, folgen, dass

$$sQ \equiv tQ \pmod{p},$$

und, da Q relative Primzahl zu p ist, auch

$$s \equiv t \pmod{p}$$

wäre; ähnlich würde aus derselben Annahme gleichzeitig

$$s' \equiv t' \pmod{p'}; \quad s'' \equiv t'' \pmod{p''} \ldots$$

folgen, so dass also die beiden Combinationen s, s', s'' ... und t, t', t'' ... identisch wären. In der That durchläuft also m ein vollständiges Restsystem in Bezug auf den Modulus P. Ferner ist nun

$$\left(\frac{m}{p}\right) = \left(\frac{sQ + s'Q' + s''Q'' + \cdots}{p}\right) = \left(\frac{sQ}{p}\right) = \left(\frac{s}{p}\right)\left(\frac{Q}{p}\right),$$

und ebenso

$$\left(\frac{m}{p'}\right) = \left(\frac{s'}{p'}\right)\left(\frac{Q'}{p'}\right), \quad \left(\frac{m}{p''}\right) = \left(\frac{s''}{p''}\right)\left(\frac{Q''}{p''}\right)\cdots,$$

folglich auch, wenn man alle diese Gleichungen multiplicirt,

$$\left(\frac{m}{P}\right) = \left(\frac{s}{p}\right)\left(\frac{s'}{p'}\right)\left(\frac{s''}{p''}\right)\cdots\left(\frac{Q}{p}\right)\left(\frac{Q'}{p'}\right)\left(\frac{Q''}{p''}\right)\cdots$$

Multiplicirt man daher beide Seiten der obigen Gleichung (2) mit

$$\left(\frac{Q}{p}\right)\left(\frac{Q'}{p'}\right)\left(\frac{Q''}{p''}\right)\cdots,$$

so erhält man

$$\Sigma\left(\frac{m}{P}\right)e^{m\frac{2h\pi i}{P}} = \left(\frac{Q}{p}\right)\left(\frac{Q'}{p'}\right)\left(\frac{Q''}{p''}\right)\cdots\left(\frac{h}{P}\right)i^{\Sigma^1/_4(p-1)^2}\sqrt{P},$$

wo rechts zur Abkürzung

$$\left(\frac{p-1}{2}\right)^2 + \left(\frac{p'-1}{2}\right)^2 + \left(\frac{p''-1}{2}\right)^2 + \cdots = \Sigma\left(\frac{p-1}{2}\right)^2$$

gesetzt ist. Da nun ferner

$$\left(\frac{Q}{p}\right) = \left(\frac{p'}{p}\right)\left(\frac{p''}{p}\right)\cdots$$
$$\left(\frac{Q'}{p'}\right) = \left(\frac{p}{p'}\right)\left(\frac{p''}{p'}\right)\cdots$$
$$\left(\frac{Q''}{p''}\right) = \left(\frac{p}{p''}\right)\left(\frac{p'}{p''}\right)\cdots$$
$$\cdots\cdots\cdots\cdots\cdots$$

ist, so erhält man durch Multiplication

$$\left(\frac{Q}{p}\right)\left(\frac{Q'}{p'}\right)\left(\frac{Q''}{p''}\right)\cdots = \Pi\left(\frac{p}{p'}\right)\left(\frac{p'}{p}\right),$$

wo das Productzeichen Π sich auf alle möglichen Paare von je zwei verschiedenen Primzahlen p, p' bezieht. Da nun nach dem Reciprocitätssatze

$$\left(\frac{p}{p'}\right)\left(\frac{p'}{p}\right) = (-1)^{\frac{1}{2}(p-1)\cdot\frac{1}{2}(p'-1)} = i^{\frac{1}{2}(p-1)(p'-1)}$$

ist, so erhält man

$$\left(\frac{Q}{p}\right)\left(\frac{Q'}{p'}\right)\left(\frac{Q''}{p''}\right)\cdots = i^{2\Sigma\frac{1}{2}(p-1)\cdot\frac{1}{2}(p'-1)},$$

wo das Summenzeichen rechter Hand sich wieder auf alle Combinationen von je zwei verschiedenen Primzahlen p, p' bezieht; es ist ferner

$$\Sigma\left(\frac{p-1}{2}\right)^2 + 2\,\Sigma\,\frac{p-1}{2}\,\frac{p'-1}{2}$$
$$= \left(\frac{p-1}{2} + \frac{p'-1}{2} + \frac{p''-1}{2} + \cdots\right)^2,$$

folglich

$$\Sigma\left(\frac{m}{P}\right)e^{m\frac{2h\pi i}{P}} = \left(\frac{h}{P}\right)i^{[\frac{1}{2}(p-1)+\frac{1}{2}(p'-1)+\cdots]^2}\sqrt{P}.$$

Da endlich (vergl. §. 46)

$$P = (1+(p-1))(1+(p'-1))(1+(p''-1))\cdots$$
$$\equiv 1+(p-1)+(p'-1)+(p''-1)+\cdots \pmod 4$$

und folglich

$$\frac{P-1}{2} \equiv \frac{p-1}{2} + \frac{p'-1}{2} + \frac{p''-1}{2} + \cdots \pmod 2$$

und hieraus

$$\left(\frac{P-1}{2}\right)^2 \equiv \left(\frac{p-1}{2} + \frac{p'-1}{2} + \frac{p''-1}{2}\cdots\right)^2 \pmod 4$$

ist, so ergiebt sich schliesslich

$$\Sigma\left(\frac{m}{P}\right)e^{m\frac{2h\pi i}{P}} = \left(\frac{h}{P}\right)i^{\frac{1}{4}(P-1)^2}\sqrt{P},$$

worin der zu beweisende Satz besteht. Nimmt man $h \equiv 0 \pmod P$, so erhält man wieder den (in §. 52. I. bewiesenen) Satz

$$\Sigma\left(\frac{m}{P}\right) = 0.$$

II. Ueber den Grenzwerth einer unendlichen Reihe.

§. 117.

Lehrsatz: Sind a und b zwei positive Constanten, so convergirt die unendliche Reihe

$$S = \frac{1}{b^{1+\varrho}} + \frac{1}{(b+a)^{1+\varrho}} + \frac{1}{(b+2a)^{1+\varrho}} + \frac{1}{(b+3a)^{1+\varrho}} + \cdots$$

für jeden positiven Werth von ϱ, und bei unbegrenzter Abnahme dieser positiven Zahl ϱ nähert sich das Product ϱS dem Grenzwerthe a^{-1}.

Beweis. Construiren wir für einen bestimmten positiven Werth von ϱ die Curve, deren Gleichung in Bezug auf ein rechtwinkliges Coordinatensystem

$$y = \frac{1}{x^{1+\varrho}}$$

ist, so hat die Fläche, welche zwischen ihr und der unendlichen positiven Abscissenaxe liegt, von $x = b$ an gerechnet, den endlichen Werth

$$\int_b^{+\infty} y\,dx = \frac{1}{\varrho\, b^{\varrho}}.$$

Die Ordinaten der Curve, welche den Abscissen

$$b,\ b+a,\ b+2a,\ b+3a \ldots$$

entsprechen, sind

$$\frac{1}{b^{1+\varrho}}, \quad \frac{1}{(b+a)^{1+\varrho}}, \quad \frac{1}{(b+2a)^{1+\varrho}}, \quad \frac{1}{(b+3a)^{1+\varrho}} \cdots;$$

ihre Fusspuncte sind äquidistant und zerlegen die Abscissenaxe in unendlich viele Stücke von der Grösse a. Construirt man über jedem dieser Stücke als Grundlinie ein Rechteck, dessen Höhe gleich der letzten Ordinate in diesem Stück ist, so haben diese Rechtecke der Reihe nach den Flächeninhalt

$$\frac{a}{(b+a)^{1+\varrho}}, \quad \frac{a}{(b+2a)^{1+\varrho}}, \quad \frac{a}{(b+3a)^{1+\varrho}} \cdots$$

Da nun die Ordinate y der Curve mit stetig wachsendem x stetig abnimmt, so ist jedes dieser Rechtecke kleiner als der über demselben Abscissenstück liegende, bis zur Curve ausgedehnte Flächenstreifen, und folglich ist die Summe von noch so vielen jener Rechtecke stets kleiner als die gesammte, oben von der Curve begrenzte Fläche; d. h. es ist

$$\frac{a}{(b+a)^{1+\varrho}} + \frac{a}{(b+2a)^{1+\varrho}} + \frac{a}{(b+3a)^{1+\varrho}} + \cdots < \frac{1}{\varrho b^{\varrho}},$$

oder es ist, wenn auf beiden Seiten $ab^{-1-\varrho}$ addirt wird,

$$aS < \frac{1}{\varrho b^{\varrho}} + \frac{a}{b^{1+\varrho}},$$

woraus folgt, dass die aus lauter positiven Gliedern bestehende Reihe S wirklich für jeden positiven Werth von ϱ convergirt.

Construirt man nun über jedem der obigen Abscissenstücke als Grundlinie ein zweites Rechteck, dessen Höhe gleich der ersten Ordinate in diesem Stück ist, so sind diese Rechtecke, deren Flächeninhalt gleich

$$\frac{a}{b^{1+\varrho}}, \quad \frac{a}{(b+a)^{1+\varrho}}, \quad \frac{1}{(b+2a)^{1+\varrho}} \cdots,$$

nothwendig grösser als die über denselben Stücken liegenden, bis zur Curve fortgesetzten Flächenstreifen, aus dem schon oben angeführten Grunde, weil mit wachsendem x die Ordinate y stetig abnimmt. Die Summe aller dieser Rechtecke ist daher grösser als die gesammte, oben von der Curve begrenzte Fläche, d. h. es ist

$$aS > \frac{1}{\varrho b^{\varrho}}.$$

Auf diese Weise ist der Werth der unendlichen Reihe S und folglich auch der des Productes ϱS in zwei Grenzen eingeschlossen; es ist nämlich

$$\frac{1}{a\,b^{\varrho}} < \varrho S < \frac{1}{a\,b^{\varrho}} + \frac{\varrho}{b^{1+\varrho}}.$$

Wenn nun der positive Werth ϱ unendlich klein wird, so nähert sich sowohl

$$\frac{1}{a\,b^{\varrho}}, \text{ als auch } \frac{1}{a\,b^{\varrho}} + \frac{\varrho}{b^{1+\varrho}}$$

einem und demselben Grenzwerth a^{-1}; mithin muss auch das Product ϱS sich demselben Grenzwerth a^{-1} nähern, was zu beweisen war.

§. 118.

Der so eben bewiesene Satz bildet nur einen speciellen Fall des folgenden, welcher seiner zahlreichen Anwendungen wegen von der grössten Wichtigkeit ist:

Es sei K ein System von positiven Zahlwerthen k, und T diejenige unstetige Function von einer positiven stetigen Veränderlichen t, welche angiebt, wie viele der in K enthaltenen Zahlwerthe k den Werth t nicht übertreffen; wenn nun mit unendlich wachsendem t der Quotient $T : t$ sich einem bestimmten endlichen Grenzwerthe ω nähert, so convergirt die Reihe

$$S = \sum \frac{1}{k^{1+\varrho}}$$

für jeden positiven Werth von ϱ, und das Product ϱS nähert sich mit unendlich abnehmendem ϱ demselben Grenzwerthe ω.

Es wird gut sein, dem Beweise dieses allgemeinen Princips*) einige erläuternde Bemerkungen voranzuschicken. Zufolge der Bedeutung von T entspricht jedem endlichen Werthe von t auch

*) *Dirichlet: Recherches* etc. §. 1. — *Dirichlet: Sur un théorème relatif aux séries*, Crelle's Journal Bd. LIII.

ein endlicher Werth von T; denn wären in K unendlich viele Zahlen k enthalten, welche den endlichen Werth t nicht übertreffen, so würde auch jedem grössern Werthe von t eine unendliche Anzahl T entsprechen; es würde daher das Verhältniss $T : t$ fortwährend unendlich gross sein; dies widerspricht aber der Annahme, dass $T : t$ sich einem endlichen Grenzwerth ω mit wachsendem t nähert. Es leuchtet ferner ein, dass die ganze Zahl T nur dann ihren Werth ändert, wenn t einen Werth erreicht, welcher einer oder mehreren einander gleichen in K enthaltenen Zahlen k gleich ist, und zwar wird T dann plötzlich um ebenso viele Einheiten zunehmen, als es Zahlen k giebt, welche diesem Werth t gleich sind.

In dem einfachsten Falle, wenn K nur aus einer endlichen Anzahl von Zahlwerthen k besteht, leuchtet die Richtigkeit des obigen Satzes unmittelbar ein; denn sobald t dem grössten dieser Werthe k gleich geworden ist, bleibt T bei weiter wachsendem t unverändert; es ist folglich $\omega = 0$; und da andererseits die Summe

$$\Sigma \frac{1}{k}$$

einen endlichen Werth hat, so wird auch das Product ϱS mit unendlich kleinem ϱ ebenfalls unendlich klein werden.

Ebenso bestätigt sich der allgemeine Satz in dem speciellen Falle, welcher in dem vorigen Paragraphen behandelt ist. Das System K besteht dort aus den sämmtlichen Zahlen von der Form $b + na$, die den sämmtlichen Werthen $0, 1, 2, 3 \ldots$ von n entsprechen; wenn nun $t = b + na$ oder $> b + na$, aber $< b + (n+1)a$ ist, so ist entsprechend $T = n + 1$, und folglich nähert sich der Quotient $T : t$ mit unendlich wachsendem t, also auch mit unendlich wachsendem n dem Grenzwerth

$$\omega = \frac{1}{a};$$

und in der That haben wir gefunden, dass dieser Werth auch zugleich der Grenzwerth des Productes ϱS ist, wenn die positive Grösse ϱ unendlich klein wird.

§. 119.

Wir gehen nun zu dem Beweise des allgemeinen Satzes über und beginnen damit, die in K enthaltenen Zahlwerthe k ihrer Grösse nach zu ordnen und mit Indices zu versehen, in der Weise, dass

$$k_1 \leqq k_2 \leqq k_3 \leqq k_4 \leqq k_5 \ldots$$

wird; dies ist offenbar möglich, da unterhalb eines beliebigen endlichen positiven Werthes t immer nur eine endliche Anzahl von Zahlwerthen k vorhanden ist; sind mehrere Zahlen k gleich gross, so muss jede einzelne ihren besondern Index erhalten, so dass dann mehreren auf einander folgenden Indices gleich grosse Zahlwerthe k entsprechen.

Sehen wir ab von dem interesselosen Falle, in welchem nur eine endliche Anzahl von Werthen k vorhanden ist, so lässt sich zunächst zeigen, dass mit unbegrenzt wachsendem n auch der Quotient

$$h_n = \frac{n}{k_n}$$

sich demselben Grenzwerth ω nähert, und durch diese Bemerkung wird dann der allgemeine Satz auf den vorher (§. 117) behandelten speciellen Fall zurückgeführt.

In der That, wenn δ eine beliebig kleine positive gegebene Grösse bedeutet, so kann man entsprechend einen positiven Werth τ immer so gross wählen, dass für alle Werthe $t \geqq \tau$ die Bedingung

$$\omega - \delta < \frac{T}{t} < \omega + \delta$$

erfüllt ist. Es sei ferner ν derjenige Werth von T, welcher $t = \tau$ entspricht, also $k_\nu \leqq \tau < k_{\nu+1}$, und n irgend eine der positiven ganzen Zahlen $\nu+1, \nu+2, \nu+3 \ldots$; dann ist jedenfalls $k_n > \tau$, und wenn mehrere auf einander folgende Grössen k denselben Werth wie k_n besitzen, so sei k_{m+1} die erste, k_r die letzte von ihnen, also n eine der Zahlen $m+1, m+2 \ldots r$. Nähert sich nun t von k_m ab wachsend dem Werthe k_n immer mehr an, so bleibt $T = m$, und der Quotient $T:t$ nähert sich abnehmend unbegrenzt dem Werthe $m:k_n$, und da $m < n$ ist, so folgt, dass

$$\frac{T}{t} < h_n$$

ist, sobald t sehr nahe unterhalb k_n liegt; für $t = k_n$ wird aber $T = r \geqq n$, und folglich

$$\frac{T}{t} \geqq h_n.$$

Da nun bei diesem Wachsen von $t < k_n$ bis $t = k_n > \tau$ der Quotient $T:t$ stets zwischen $\omega - \delta$ und $\omega + \delta$ liegt, und zugleich, wie eben gezeigt ist, von Werthen, die $< h_n$ sind, auf einen Werth springt, der $\geqq h_n$ ist, so muss auch $\omega - \delta < h_n < \omega + \delta$ sein. Wie klein also auch δ sein mag, so kann n stets so gross gewählt werden, dass h_n definitiv um weniger als δ von ω verschieden wird, d. h. h_n nähert sich mit unbegrenzt wachsendem n demselben Grenzwerth ω.

Mit Hülfe dieses Resultates lässt sich der Beweis des allgemeinen Satzes leicht führen. Da nämlich

$$S = \Sigma \frac{1}{k^{1+\varrho}} = \frac{h_1^{1+\varrho}}{1^{1+\varrho}} + \frac{h_2^{1+\varrho}}{2^{1+\varrho}} + \frac{h_3^{1+\varrho}}{3^{1+\varrho}} + \cdots$$

ist, wo h_n mit unendlich wachsendem n sich dem Grenzwerthe ω nähert und folglich endlich, d. h. kleiner als eine angebbare Constante H bleibt, so ist die Summe S' der ersten n Glieder der Reihe S kleiner als das Product aus $H^{1+\varrho}$ und der Summe $\mathfrak{S}'$ der ersten n Glieder der folgenden Reihe

$$\mathfrak{S} = \frac{1}{1^{1+\varrho}} + \frac{1}{2^{1+\varrho}} + \frac{1}{3^{1+\varrho}} + \cdots;$$

da nun die letztere (nach §. 117) für jeden *positiven* Werth von ϱ convergirt, so *convergirt* auch die Reihe S. Setzt man nun $S = S' + S''$, $\mathfrak{S} = \mathfrak{S}' + \mathfrak{S}''$, so wird $S'' = h^{1+\varrho}\mathfrak{S}''$, wo h einen (jedenfalls positiven) Mittelwerth aus den Werthen $h_{n+1}, h_{n+2} \cdots$ bedeutet. Ist daher δ eine beliebig kleine positive gegebene Grösse, und n so gross gewählt (was stets möglich ist), dass alle diese Werthe zwischen $\omega - \delta$ und $\omega + \delta$ liegen, so wird auch h, und für hinreichend kleine Werthe von ϱ auch $h^{1+\varrho}$ zwischen denselben Grenzen liegen. Da ferner (nach §. 117) das Product $\varrho\mathfrak{S}''$ mit unbegrenzt abnehmendem positiven ϱ sich der Einheit unendlich annähert, so wird für hinreichend kleine Werthe von ϱ auch das Product $\varrho S'' = h^{1+\varrho} \cdot \varrho\mathfrak{S}''$ zwischen den Grenzen $\omega - \delta$ und $\omega + \delta$ liegen. Da endlich $\varrho S'$ gleichzeitig unendlich klein wird, weil S' nur

eine endliche Anzahl von Gliedern enthält, so wird für sehr kleine Werthe von ϱ auch $\varrho S = \varrho S' + \varrho S''$ zwischen denselben Grenzen $\omega - \delta$ und $\omega + \delta$ liegen. Hiermit ist also auch bewiesen, dass mit unbegrenzt abnehmendem ϱ das Product ϱS *sich dem Grenzwerthe* ω *unendlich annähert**).

---

*) Es verdient bemerkt zu werden, dass man den obigen allgemeinen Satz nicht umkehren darf. Besteht z. B. das System K aus einer Zahl $k = 1$, aus $(\theta - 1)$ Zahlen $k = \theta$, aus $(\theta^2 - \theta)$ Zahlen $k = \theta^2$, aus $(\theta^3 - \theta^2)$ Zahlen $k = \theta^3$ u. s. f., wo θ eine positive ganze Zahl > 1 bedeutet, so ist für jeden positiven Werth von ϱ

$$S = 1 + \frac{\theta - 1}{\theta(\theta\varrho - 1)},$$

und das Product ϱS nähert sich mit unendlich abnehmendem ϱ dem Grenzwerthe

$$\omega = \frac{\theta - 1}{\theta \log \theta},$$

während der Quotient $T : t$ bei unendlich wachsendem t fortwährend von dem Werth 1 abnehmend durch ω hindurch geht bis zu dem Werth $1 : \theta$, dann aber sogleich wieder zu dem Werth 1 zurückspringt, um von Neuem denselben Veränderungsprocess zu erleiden (vergl. §. 144).

III. Ueber einen geometrischen Satz.

§. 120.

In einer Ebene sei eine vollständig begrenzte Figur F von allenthalben endlichen Dimensionen construirt, deren Flächeninhalt wir mit A bezeichnen wollen. Sind ferner X und Y zwei auf einander senkrechte Axen, und construirt man parallel mit ihnen zwei Systeme äquidistanter Parallelen, welche ein über die ganze Ebene ausgebreitetes Gitter bilden, so wird, wenn δ der Abstand je zweier benachbarter Parallelen, und T die Anzahl der Gitterpuncte ist, welche innerhalb F liegen, das Product $T\delta^2$ mit unendlich abnehmendem δ sich dem Grenzwerthe A nähern*).

Um diesen Satz zu beweisen, betrachten wir das System der mit Y parallelen Geraden und nehmen der Einfachheit halber an, dass jede derselben die Begrenzung der Figur nur zweimal schneidet; bezeichnen wir mit h die Länge des innerhalb F liegenden Stückes irgend einer solchen Parallelen, so ist $h\delta$ nahezu der Flächeninhalt des zwischen dieser und der folgenden Parallelen enthaltenen Theiles der Fläche F, und es wird in der Lehre von der Quadratur bewiesen, dass die Summe aller dieser Rechtecke $h\delta$ sich mit unendlich abnehmendem δ dem wahren Flächeninhalt A der Figur unbegrenzt nähert. Bezeichnen wir nun mit n die Anzahl der auf h liegenden Gitterpuncte (wobei es gleichgültig ist, ob ein zufällig auf der Begrenzung von F liegender Gitterpunct mitgezählt oder ausgeschlossen wird), so besteht h aus $(n-1)$ Stücken $= \delta$ und aus einem Rest, welcher höchstens $= 2\delta$ ist,

*) *Dirichlet: Recherches* etc. §. 1.

so dass wir $h = n\delta + \varepsilon\delta$ setzen können, wo ε einen positiven oder negativen echten Bruch bedeutet. Es ist daher

$$\Sigma\, h\delta = \Sigma\,(n\delta^2 + \varepsilon\delta^2) = T\delta^2 + \delta\,\Sigma\,\varepsilon\delta;$$

es ist ferner, da ε absolut genommen höchstens $= 1$ ist, die Summe $\Sigma\,\varepsilon\delta$ höchstens gleich der endlichen Ausdehnung der Figur F in der Richtung der Axe X, und es wird daher $\delta\,\Sigma\,\varepsilon\delta$ mit δ gleichzeitig unendlich klein. Folglich nähert sich das Product $T\delta^2$ demselben Grenzwerthe A, welchem sich $\Sigma\, h\delta$ nähert; was zu beweisen war.

Es leuchtet übrigens ein, dass dieser Satz nicht an die Beschränkung gebunden ist, nach welcher die Parallelen mit der Axe Y nur einmal in die Figur F ein- und nur einmal aus ihr austreten. Man kann immer die Figur F als ein Aggregat von positiven und negativen Flächentheilen ansehen, welche einzeln der angegebenen Bedingung genügen; und wendet man auf jeden einzelnen Theil den Satz an, so ergiebt sich daraus sofort die Richtigkeit desselben für die ganze Figur F.

IV. Ueber die Geschlechter, in welche die Classen der quadratischen Formen von bestimmter Determinante zerfallen*).

§. 121.

Ist (a, b, c) eine quadratische Form von der Determinante $b^2 - ac = D$, und sind z, z' irgend zwei durch diese Form darstellbare Zahlen (wobei es gleichgültig ist, ob die darstellenden Zahlen relative Primzahlen sind oder nicht), so lässt sich das Product zz' stets in die Form $x^2 - Dy^2$ bringen, wo x und y ganze Zahlen bedeuten; denn aus der Annahme

$$z = a\alpha^2 + 2b\alpha\gamma + c\gamma^2, \quad z' = a\beta^2 + 2b\beta\delta + c\delta^2$$

folgt (nach §. 54), dass die Form (a, b, c) durch die Substitution $\left(\begin{smallmatrix}\alpha, & \beta\\ \gamma, & \delta\end{smallmatrix}\right)$ in eine Form (z, x, z') übergeht, deren Determinante $x^2 - zz'$ von der Form Dy^2 ist. Aus dieser Bemerkung lassen sich folgende Schlüsse ziehen**).

1. Ist l eine ungerade in D aufgehende Primzahl, so hat für alle durch l nicht theilbaren Zahlen n, welche durch die Form (a, b, c) darstellbar sind, das Symbol

$$\left(\frac{n}{l}\right)$$

einen und denselben Werth. Denn sind n und n' irgend zwei solche durch l nicht theilbare und durch (a, b, c) darstellbare

*) *Dirichlet: Recherches sur diverses applications* etc. §§. 3, 6 (Crelle's Journal XIX).

**) Vergl. *Gauss: D. A.* artt. 229—231.

Zahlen, so folgt aus $nn' = x^2 - Dy^2$, dass $nn' \equiv x^2 \pmod{l}$, und folglich

$$\left(\frac{nn'}{l}\right) = +1, \quad \text{also} \quad \left(\frac{n}{l}\right) = \left(\frac{n'}{l}\right)$$

ist.

2. Ist $D \equiv 3 \pmod 4$, so hat für alle ungeraden durch die Form darstellbaren Zahlen n der Ausdruck

$$(-1)^{\frac{1}{2}(n-1)}$$

einen und denselben Werth. Denn sind n und n' irgend zwei solche ungerade Zahlen, so ist

$$nn' = x^2 - Dy^2 \equiv x^2 + y^2 \pmod 4;$$

da ferner nn' eine ungerade Zahl ist, so muss eine der beiden Zahlen x, y gerade, die andere ungerade sein; hieraus folgt $nn' \equiv 1 \pmod 4$, also auch $n \equiv n' \pmod 4$, und hieraus

$$(-1)^{\frac{1}{2}(n-1)} = (-1)^{\frac{1}{2}(n'-1)}.$$

3. Ist $D \equiv 2 \pmod 8$, so hat für alle durch dieselbe Form darstellbaren ungeraden Zahlen n der Ausdruck

$$(-1)^{\frac{1}{8}(n^2-1)}$$

einen und denselben Werth. Denn aus

$$nn' = x^2 - Dy^2 \equiv x^2 - 2y^2 \pmod 8$$

folgt, da x ungerade ist, $nn' \equiv \pm 1 \pmod 8$, also auch $n \equiv \pm n' \pmod 8$, woraus die obige Behauptung sich unmittelbar ergiebt.

4. Ist $D \equiv 6 \pmod 8$, so hat für alle durch dieselbe Form darstellbaren ungeraden Zahlen n der Ausdruck

$$(-1)^{\frac{1}{2}(n-1)+\frac{1}{8}(n^2-1)}$$

einen und denselben Werth. Denn aus

$$nn' = x^2 - Dy^2 \equiv x^2 + 2y^2 \pmod 8$$

folgt, da x ungerade ist, $nn' \equiv 1$ oder $\equiv 3 \pmod 8$, je nachdem y gerade oder ungerade ist; dann ist entsprechend $n \equiv n'$ oder $\equiv 3n' \pmod 8$, und man findet leicht, dass in beiden Fällen

$$\frac{n-1}{2} + \frac{n^2-1}{8} \equiv \frac{n'-1}{2} + \frac{n'^2-1}{8} \pmod 2$$

ist, was zu beweisen war.

5. Ist $D \equiv 4 \pmod 8$, so hat für alle durch dieselbe Form darstellbaren ungeraden Zahlen n der Ausdruck

$$(-1)^{\frac{1}{2}(n-1)}$$

einen und denselben Werth. Denn aus $nn' = x^2 - Dy^2$ folgt, da x ungerade ist, $nn' \equiv 1 \pmod 4$, also $n \equiv n' \pmod 4$.

6. Ist $D \equiv 0 \pmod 8$, so hat für alle durch dieselbe Form darstellbaren ungeraden Zahlen n jeder der beiden Ausdrücke

$$(-1)^{\frac{1}{2}(n-1)} \quad \text{und} \quad (-1)^{\frac{1}{8}(n^2-1)}$$

für sich einen unveränderlichen Werth. Denn aus

$$nn' = x^2 - Dy^2 \equiv x^2 \equiv 1 \pmod 8$$

folgt $n \equiv n' \pmod 8$.

§. 122.

Auf den Sätzen des vorigen Paragraphen beruht die Eintheilung der quadratischen Formen einer gegebenen Determinante D in *Geschlechter*; wir beschränken uns hier auf die *ursprünglichen* Formen, weil das, was für sie gilt, leicht auf die anderen Formen übertragen werden kann; ausserdem betrachten wir für den Fall einer negativen Determinante nur *positive*, d. h. solche Formen, deren äussere Coefficienten positiv sind. Es sei also (a, b, c) eine ursprüngliche Form der σten Art (§. 61), so wissen wir (§. 93), dass man den Variabeln derselben stets solche Werthe x, y beilegen kann, dass

$$\frac{ax^2 + 2bxy + cy^2}{\sigma} = n$$

positiv und relative Primzahl zu $2D$ wird; dabei ist es gleichgültig, ob x und y relative Primzahlen zu einander sind oder nicht. Bezeichnet man nun mit $l, l', l'' \ldots$ alle von einander verschiedenen in D aufgehenden ungeraden Primzahlen, so hat für alle durch eine und dieselbe Form (a, b, c) erzeugten Zahlen σn jedes der Symbole

$$\left(\frac{\sigma n}{l}\right), \left(\frac{\sigma n}{l'}\right), \left(\frac{\sigma n}{l''}\right) \cdots$$

und folglich auch jedes der Symbole

$$\left(\frac{n}{l}\right), \left(\frac{n}{l'}\right), \left(\frac{n}{l''}\right) \cdots$$

für sich einen unveränderlichen Werth; ist ferner D nicht $\equiv 1$ (mod. 4), also $\sigma = 1$, so gilt dasselbe, je nachdem $D \equiv 3$ (mod. 4), $D \equiv 2$ (mod. 8), $D \equiv 6$ (mod. 8), $D \equiv 4$ (mod. 8), $D \equiv 0$ (mod. 8) ist, entsprechend von dem Ausdruck

$$(-1)^{\frac{1}{8}(\quad -1)}, \quad (-1)^{\frac{1}{8}(n^2-1)}, \quad (-1)^{\frac{1}{2}(n-1)+\frac{1}{8}(n^2-1)}, \quad (-1)^{\frac{1}{2}(n-1)}$$

oder von jedem der beiden Ausdrücke

$$(-1)^{\frac{1}{2}(n-1)} \text{ und } (-1)^{\frac{1}{8}(n^2-1)}.$$

Die Anzahl dieser Ausdrücke

$$\left(\frac{n}{l}\right), \left(\frac{n}{l'}\right) \cdots (-1)^{\frac{1}{2}(n-1)} \text{ u. s. w.,}$$

die wir die *Charaktere* C nennen wollen, hängt nur von der Determinante D ab und soll im Folgenden immer mit λ bezeichnet werden; offenbar ist λ gleich der Anzahl der in D aufgehenden ungeraden Primzahlen $l, l', l'' \ldots$, wenn $D \equiv 1$ (mod. 4); in den übrigen Fällen mit Ausnahme von $D \equiv 0$ (mod. 8) ist sie um 1 und im Falle $D \equiv 0$ (mod. 8) ist sie um 2 grösser. Das System der bestimmten Werthe ± 1, welche diesen λ Charakteren C für eine bestimmte Form (a, b, c) zukommen, wollen wir den *Total-Charakter* dieser Form nennen. Nach dem Ausfall dieses Total-Charakters theilen wir sämmtliche ursprüngliche Formen von gleicher Determinante und gleicher Art in *Geschlechter* ein, indem wir je zwei Formen in dasselbe Geschlecht oder in zwei verschiedene Geschlechter werfen, je nachdem der Total-Charakter der einen Form mit dem der andern identisch ist, oder nicht; ein Geschlecht ist hiernach der Inbegriff aller ursprünglichen Formen von gleicher Determinante und gleicher Art, für welche jeder der λ Charaktere C für sich genommen denselben Werth besitzt. Da nun alle Zahlen σn, welche durch eine bestimmte Form darstellbar sind, auch durch alle mit ihr äquivalenten Formen dargestellt werden können, so gehören alle Formen einer und derselben *Classe* auch in ein und dasselbe *Geschlecht*; ein Geschlecht ist daher immer der Inbegriff einer bestimmten Anzahl von Formen-Classen. Da ferner jeder der λ Charaktere C zwei einander entgegengesetzte Werthe haben kann, so leuchtet ein, dass die sämmtlichen ursprünglichen Formen von einer gegebenen Determinante D und von der σten Art *höchstens* 2^λ verschiedene Genera bilden können.

Wir bemerken nun noch, dass die äussern Coefficienten einer Form immer durch diese Form dargestellt werden, wenn man der

einen Variabeln den Werth 1, der andern den Werth 0 beilegt; mithin können die Charaktere dieser Form immer aus einem dieser beiden Coefficienten erkannt werden.

Beispiel 1: Für die Determinante $D = -35 \equiv 1 \pmod 4$ bilden (§. 67) die sechs Formen

$$(1, 0, 35),\quad (5, 0, 7),\quad (3, \pm 1, 12),\quad (4, \pm 1, 9)$$

ein vollständiges System nicht äquivalenter (positiver) Formen der ersten Art, und die beiden Formen

$$(2, 1, 18),\quad (6, 1, 6)$$

ein solches Formensystem der zweiten Art. Um diese Formen (oder die durch sie repräsentirten Classen) in Geschlechter einzutheilen, haben wir die beiden Charaktere

$$\left(\frac{n}{5}\right) \quad \text{und} \quad \left(\frac{n}{7}\right)$$

zu betrachten, und da $\lambda = 2$ ist, so sind für jede der beiden Formenarten *höchstens vier* Geschlechter zu erwarten. Die wirkliche Untersuchung ergiebt als Resultat folgende Tabelle

(a, b, c)	$\left(\frac{n}{5}\right)$	$\left(\frac{n}{7}\right)$
$(1, 0, 35)$	$+$	$+$
$(5, 0, 7)$	$-$	$-$
$(3, \pm 1, 12)$	$-$	$-$
$(4, \pm 1, 9)$	$+$	$+$
$(2, 1, 18)$	$+$	$+$
$(6, 1, 6)$	$-$	$-$

Es zeigt sich also, dass jedes der beiden Systeme nur in *zwei* verschiedene Geschlechter zerfällt; die drei Formen

$$(1, 0, 35),\quad (4, \pm 1, 9)$$

bilden ein Geschlecht, dessen Total-Charakter durch

$$\left(\frac{n}{5}\right) = +1,\quad \left(\frac{n}{7}\right) = +1$$

bestimmt ist; die drei anderen Formen

$$(5, 0, 7), \quad (3, \pm 1, 12)$$

bilden ein zweites Geschlecht, dessen Total-Charakter durch

$$\left(\frac{n}{5}\right) = -1, \quad \left(\frac{n}{7}\right) = -1$$

bestimmt ist. Und jede der beiden Formen der zweiten Art bildet ein Geschlecht für sich.

Beispiel 2: Für die Determinante $D = -5 \equiv 3 \pmod 4$ bilden (§. 71) die beiden Formen

$$(1, 0, 5), \quad (2, 1, 3)$$

ein vollständiges System nicht äquivalenter (positiver) Formen; um sie in Geschlechter einzutheilen, müssen wir die beiden Charaktere

$$(-1)^{\frac{1}{2}(n-1)} \text{ und } \left(\frac{n}{5}\right)$$

betrachten. Der Form (1, 0, 5) entspricht

$$(-1)^{\frac{1}{2}(n-1)} = +1, \quad \left(\frac{n}{5}\right) = +1,$$

und der Form (2, 1, 3) entspricht

$$(-1)^{\frac{1}{2}(n-1)} = -1, \quad \left(\frac{n}{5}\right) = -1.$$

Jede dieser beiden Formen bildet also ein Geschlecht für sich; da $\lambda = 2$ ist, so ist auch hier die Anzahl der Geschlechter nicht $= 2^\lambda$, sondern nur $= 2^{\lambda-1}$.

Beispiel 3: Für die Determinante $D = 24 \equiv 0 \pmod 8$ findet man leicht (nach §§. 75, 78, 82), dass folgende vier Formen

$$(1, 4, -8), \quad (-1, 4, 8), \quad (3, 3, -5), \quad (-3, 3, 5)$$

ein vollständiges Formensystem bilden; es sind hier die folgenden drei Charaktere zu betrachten:

$$(-1)^{\frac{1}{2}(n-1)}, \quad (-1)^{\frac{1}{8}(n^2-1)}, \quad \left(\frac{n}{3}\right);$$

der ersten der obigen Formen entspricht

$$(-1)^{\frac{1}{2}(n-1)} = +1, \quad (-1)^{\frac{1}{8}(n^2-1)} = +1, \quad \left(\frac{n}{3}\right) = +1;$$

der zweiten

$$(-1)^{\frac{1}{2}(n-1)} = -1, \quad (-1)^{\frac{1}{8}(n^2-1)} = +1, \quad \left(\frac{n}{3}\right) = -1;$$

der dritten

$$(-1)^{\frac{1}{2}(n-1)} = -1, \quad (-1)^{\frac{1}{8}(n^2-1)} = -1, \quad \left(\frac{n}{3}\right) = +1;$$

und der vierten

$$(-1)^{\frac{1}{2}(n-1)} = +1, \quad (-1)^{\frac{1}{8}(n^2-1)} = -1, \quad \left(\frac{n}{3}\right) = -1.$$

Auch hier zeigt sich also, dass die Anzahl der wirklich vorhandenen Geschlechter nicht $= 2^\lambda$, sondern nur $= 2^{\lambda-1}$ ist.

§. 123.

Mit Hülfe des Reciprocitätssatzes lässt sich nun in der That nachweisen, dass die Anzahl der verschiedenen Geschlechter *höchstens* $= 2^{\lambda-1}$ ist. Wir setzen $D = D'S^2$, wo S^2 das grösste in D aufgehende Quadrat bezeichnet, und legen den Buchstaben δ, ε, P dieselbe Bedeutung in Bezug auf D' bei, welche sie in §. 52 in Bezug auf die dort mit D bezeichnete Zahl erhalten haben. Dann wird

$$\left(\frac{D}{n}\right) = \left(\frac{D'}{n}\right) = \delta^{\frac{1}{2}(n-1)}\, \varepsilon^{\frac{1}{8}(n^2-1)} \left(\frac{n}{P}\right),$$

wo n jede beliebige positive ganze Zahl bedeutet, die relative Primzahl zu $2D$ ist. Da nun die Determinante D keine Quadratzahl, also D' nicht $= 1$ ist, so kann auch nicht gleichzeitig $\delta = +1$, $\varepsilon = +1$ und $P = 1$ sein, und hieraus folgt leicht, dass der Ausdruck

$$\delta^{\frac{1}{2}(n-1)}\, \varepsilon^{\frac{1}{8}(n^2-1)} \left(\frac{n}{P}\right)$$

entweder mit einem der Charaktere C, oder mit dem Producte aus mehreren dieser Charaktere identisch ist; bezeichnen wir diese Charaktere mit C' und ihr Product mit $\Pi C'$, so ist also stets

$$\Pi C' = \left(\frac{D}{n}\right),$$

sobald n positiv und relative Primzahl zu $2D$ ist. Da nun durch jede ursprüngliche Form der σten Art stets Zahlen σn dargestellt werden können, in welchen n dieser Bedingung genügt (§. 93), und zwar solche Zahlen σn, von welchen D quadratischer Rest ist

(§. 60), so ergiebt sich, dass der Total-Charakter einer jeden Form so beschaffen ist, dass stets

$$\Pi C' = +1$$

und niemals $\Pi C' = -1$ wird. Da nun unter den sämmtlichen 2^λ Zeichencombinationen, welche man erhält, wenn man jedem der λ Charaktere C sowohl den Werth $+1$ wie den Werth -1 beilegt, offenbar die Hälfte so beschaffen ist, dass $\Pi C' = -1$ wird, so folgt, dass diesen Zeichencombinationen oder Total-Charakteren keine wirklich existirenden Formen entsprechen können. Mithin ist die Anzahl der wirklich existirenden Geschlechter *höchstens* $= 2^{\lambda-1}$.

Im Folgenden soll nun bewiesen werden, dass allen denjenigen Total-Charakteren, welche in Uebereinstimmung mit der oben angegebenen Relation sind, wirklich existirende Formen entsprechen, dass also die Anzahl der wirklich vorhandenen Geschlechter $= 2^{\lambda-1}$ ist, und ausserdem, dass jedes Geschlecht eine gleiche Anzahl von Formen-Classen enthält.

§. 124.

Wir wollen wieder (wie in §. 89) mit n alle positiven ganzen Zahlen bezeichnen, die relative Primzahlen zu $2D$ sind, ferner mit m alle diejenigen Zahlen n, von welchen D quadratischer Rest ist, und mit μ die Anzahl der von einander verschiedenen in m aufgehenden Primzahlen. Es sei ferner $\psi(n)$ eine der Bedingung $\psi(n')\,\psi(n'') = \psi(n'n'')$ genügende Function, so ist stets

$$\Sigma\,\psi(n^2)\,\Sigma\,2^\mu\psi(m) = \Sigma\,\psi(n)\,\Sigma\left(\frac{D}{n}\right)\psi(n),$$

vorausgesetzt, dass die hier vorkommenden unendlichen Reihen bestimmte von der Anordnung der Glieder unabhängige Werthe haben. Offenbar geht diese Gleichung durch die Specialisirung $\psi(n) = n^{-s}$ in die Endgleichung des §. 89 über, und sie könnte auch genau auf dieselbe Art wie diese bewiesen werden. Wir ziehen hier folgende Verification vor.

Verfährt man, wie in §. 91, so erhält man durch Ausführung der Multiplication der beiden unendlichen Reihen auf der rechten Seite

$$\Sigma\, \tau_n \psi(n),$$

wo

$$\tau_n = \Sigma \left(\frac{D}{\delta}\right)$$

ist, und δ alle Divisoren der Zahl n durchlaufen muss. Denkt man sich nun die Zahl n dargestellt als Product von Primzahlpotenzen $A, B \ldots$ und bezeichnet man mit a alle Divisoren von A, mit b alle Divisoren von B u. s. w., so leuchtet ein, dass τ_n das Product aus den Summen

$$\Sigma \left(\frac{D}{a}\right), \quad \Sigma \left(\frac{D}{b}\right) \cdots$$

ist. Wenn nun z. B. $A = q^\alpha$, und q eine Primzahl ist, so wird

$$\Sigma \left(\frac{D}{a}\right) = \alpha + 1,$$

wenn D quadratischer Rest von q ist; ist dagegen D Nichtrest von q, so wird

$$\Sigma \left(\frac{D}{a}\right) = 1 \quad \text{oder} \quad = 0,$$

je nachdem α gerade oder ungerade, d. h. je nachdem A ein Quadrat oder kein Quadrat ist. Bezeichnet man daher mit k alle diejenigen Zahlen n, in welchen nur solche Primfactoren aufgehen, von denen D Nichtrest ist, so folgt hieraus, dass jede Zahl n, für welche τ_n von Null verschieden ausfällt, von der Form mk^2 ist; und zwar ist dann τ_n gleich der Anzahl τ_m aller Divisoren von m. Da ferner $\psi(mk^2) = \psi(m)\psi(k^2)$ ist, so wird die rechte Seite unserer Gleichung gleich

$$\Sigma\, \tau_m \psi(mk^2) = \Sigma\, \psi(k^2) \cdot \Sigma\, \tau_m \psi(m).$$

Wir wenden uns nun zur linken Seite; da jede Zahl n von der Form km ist, so ergiebt sich zunächst

$$\Sigma\, \psi(n^2) = \Sigma\, \psi(k^2) \cdot \Sigma\, \psi(m^2),$$

und folglich braucht nur noch gezeigt zu werden, dass

$$\Sigma\, \psi(m^2) \Sigma\, 2^\mu \psi(m) = \Sigma\, \tau_m \psi(m)$$

ist*). Führen wir links die Multiplication aus, indem wir alle Glieder des Productes, welche denselben Factor $\psi(m)$ enthalten, in ein einziges zusammenfassen, so erhalten wir ein Resultat von der Form

$$\Sigma\, \tau'_m \psi(m),$$

*) Der gemeinschaftliche Werth beider Seiten ist das Quadrat von $\Sigma\, \psi(m)$.

wo der Coefficient

$$\tau'_m = \Sigma\, 2^\nu$$

aus ebenso vielen Gliedern besteht, als die Zahl m quadratische Divisoren δ^2 besitzt, und wo die Zahl ν für jede Zerlegung von der Form $m = \varepsilon\delta^2$ angiebt, wie viele verschiedene Primzahlen in ε aufgehen. Es braucht daher jetzt nur noch nachgewiesen zu werden, dass $\tau'_m = \tau_m$ ist, d. h. es muss folgender Satz bewiesen werden:

Zerlegt man eine ganze positive Zahl m auf alle mögliche Arten in zwei Factoren, von denen der eine ein Quadrat δ^2 ist, und bezeichnet man mit ν jedesmal die Anzahl der in dem andern Factor ε aufgehenden von einander verschiedenen Primzahlen, so ist $\Sigma\, 2^\nu$ gleich der Anzahl τ_m aller Divisoren der Zahl m.

Von der Richtigkeit dieses Satzes überzeugt man sich aber leicht auf folgende Weise. Ist

$$m = a^\alpha b^\beta c^\gamma \ldots,$$

wo $a, b, c \ldots$ von einander verschiedene Primzahlen bedeuten, so ist jeder Divisor ε von der Form

$$\varepsilon = A B C \ldots,$$

wo $A, B, C \ldots$ resp. irgend welche Glieder aus den Reihen

$$\begin{aligned} &a^\alpha,\ a^{\alpha-2},\ a^{\alpha-4} \ldots \\ &b^\beta,\ b^{\beta-2},\ b^{\beta-4} \ldots \\ &c^\gamma,\ c^{\gamma-2},\ c^{\gamma-4} \ldots \end{aligned}$$

u. s. w. bedeuten, welche so weit fortzusetzen sind, als die Exponenten nicht negativ werden. Lässt man nun jedem Factor $A, B, C \ldots$ resp. einen Factor $A', B', C' \ldots$ entsprechen, welcher $= 2$ oder $= 1$ ist, je nachdem der entsprechende Exponent > 0 oder $= 0$ ist, so wird

$$2^\nu = A' B' C' \ldots,$$

und folglich

$$\Sigma\, 2^\nu = \Sigma\, A' \cdot \Sigma\, B' \cdot \Sigma\, C' \ldots;$$

da aber, wie unmittelbar einleuchtet

$$\Sigma\, A' = \alpha + 1,\ \Sigma\, B' = \beta + 1,\ \Sigma\, C' = \gamma + 1 \ldots$$

ist, so findet man

$$\Sigma\, 2^\nu = (\alpha+1)(\beta+1)(\gamma+1)\ldots = \tau_m,$$

was zu beweisen war.

Die Richtigkeit der obigen Gleichung ist also hiermit ebenfalls erwiesen.

Bei einer aufmerksamen Prüfung der vorstehenden Ableitung wird man leicht den Zusammenhang zwischen ihr und dem (in §. 91 aufgestellten) Satze über die sämmtlichen Darstellungen einer Zahl σn durch das vollständige System S der ursprünglichen Formen der σten Art erkennen, und man wird auf diese Weise zu einem sehr einfachen Beweise dieses letztern Satzes gelangen, wenn man von dem in §. 60 oder §. 86 gewonnenen Resultat ausgeht, dass die Anzahl der verschiedenen *Gruppen* von *eigentlichen* Darstellungen einer Zahl σm durch die Formen des Systems S gleich 2^{μ} ist, wo μ die Anzahl der verschiedenen in m aufgehenden Primzahlen bedeutet.

Schliesslich bemerken wir, dass der Satz sich bedeutend verallgemeinern lässt, wenn man statt des in ihm vorkommenden Jacobi'schen Symbols irgend eine Function $\theta(n)$ einführt, welche der Bedingung $\theta(n')\,\theta(n'') = \theta(n'n'')$ genügt und nur eine *endliche* Anzahl verschiedener Werthe besitzt.

§. 125.

Nach §. 123 zerfallen die sämmtlichen (positiven) Formen von der Determinante D und von der σten Art, und also auch die sämmtlichen h Formenclassen in höchstens $\tau = 2^{\lambda-1}$ verschiedene Geschlechter, deren Total-Charaktere sämmtlich der Bedingung

$$\Pi\, C' = +1$$

genügen, und die wir mit

$$G_1,\ G_2 \ldots G_\tau$$

bezeichnen wollen; die Anzahl der Formen-Classen, welche diese Geschlechter enthalten, sollen entsprechend mit

$$g_1, g_2 \cdots g_\tau$$

bezeichnet werden, so dass also, wenn eins dieser Geschlechter, z. B. G_r, nicht wirklich vorhanden sein sollte, $g_r = 0$ zu setzen ist. Es soll nun gerade im Folgenden gezeigt werden, dass dies niemals eintritt, dass also diese τ Geschlechter wirklich existiren, und ausserdem, dass sie alle gleich viele Formen-Classen enthalten, dass also

$$g_1 = g_2 = g_3 \cdots = \frac{1}{\tau}\, h$$

ist.

Zu diesem Zweck benutzen wir die im vorigen Paragraphen bewiesene Gleichung*), indem wir

$$\psi(n) = \frac{\chi(n)}{n^s}$$

setzen, wo $\chi(n)$ irgend eins der $2^\lambda = 2\tau$ Glieder der Summe bedeutet, welche durch die Entwicklung des über alle λ Charaktere C erstreckten Productes

$$\Pi(1 + C)$$

entsteht; der Bedingung $\psi(n)\,\psi(n') = \psi(nn')$ geschieht offenbar durch jede solche Specialisirung Genüge, denn alle Factoren C, aus denen eine solche Function $\chi(n)$ zusammengesetzt ist, genügen derselben Bedingung. Da ausserdem $\chi(n)$ für jede Zahl n, die relative Primzahl zu $2D$ ist, $= \pm 1$ ist, so convergiren die vier in der Gleichung vorkommenden unendlichen Reihen unabhängig von der Anordnung ihrer Glieder für jeden positiven Werth $s > 1$. Es ist also unter dieser Annahme, da $\chi(n^2) = \chi(n)\,\chi(n) = +1$ ist,

$$\Sigma \frac{1}{n^{2s}} \Sigma \chi(m) \frac{2^\mu}{m^s} = \Sigma \frac{\chi(n)}{n^s} \Sigma \left(\frac{D}{n}\right) \frac{\chi(n)}{n^s}.$$

Denken wir uns nun wieder (wie in §. 88) ein vollständiges System S von h Formen

$$(a, b, c),\quad (a', b', c') \ldots$$

von der Determinante D und von der σten Art aufgeschrieben, und unterwerfen wir die Variabeln x, y jeder Form den dort angegebenen Bedingungen I., II., III., so wird jede Zahl σm im Ganzen auf $\varkappa \cdot 2^\mu$ verschiedene Arten erzeugt, wo $\varkappa$ die ebendaselbst festgesetzte, nur von D und σ abhängige Bedeutung hat. Die sämmtlichen h Formen des Systemes S zerfallen nun in zwei Gruppen, nämlich in eine Gruppe von H Formen, die wir mit (a, b, c) bezeichnen wollen, für welche $\chi(m) = +1$ ist, und in

*) Auch ohne Hülfe derselben gelangt man auf einem etwas kürzern, wenn auch principiell nicht verschiedenen Wege zum Ziele, wenn man von der aus §. 91 folgenden Gleichung $\varkappa_\nu \Sigma \tau_n \psi(n) = \Sigma \psi(\nu)$ ausgeht, wo ψ eine willkürliche Function, und $\sigma\nu$ alle die Zahlen bedeutet, welche durch das System der Formen (a, b, c) unter den Bedingungen I., II. des §. 90 erzeugt werden. Setzt man dann $\psi(n) = n^{-s}\,\Pi(1 + \gamma_r C)$, wo γ_r den Werth des Charakters C im Geschlechte G_r bedeutet, so wird dies letztere rechts sofort isolirt, während der Grenzprocess auf der linken Seite für jeden Bestandtheil $c_r\chi(n)$ des Productes $\Pi(1 + \gamma_r C)$ einzeln ausgeführt werden kann.

eine zweite Gruppe von H' Formen, die wir mit (a', b', c') bezeichnen wollen, für welche $\chi(m) = -1$ ist. Offenbar werden auf diese Weise alle g_r Formen des Systems S, welche einem und demselben Geschlecht G_r angehören, auch einer und derselben dieser beiden Gruppen zugetheilt; denn für alle diese Formen hat jeder Factor von $\chi(m)$ für sich genommen und folglich auch $\chi(m)$ selbst einen und denselben Werth. Und umgekehrt leuchtet ein, dass alle Zahlen σm, denen $\chi(m) = +1$ entspricht, ausschliesslich durch Formen der ersten Gruppe, und alle Zahlen σm, denen $\chi(m) = -1$ entspricht, ausschliesslich durch Formen der zweiten Gruppe erzeugt werden.

Mithin ist

$$\varkappa \sum \chi(m) \frac{2^\mu}{m^s} = \left\{ \begin{array}{l} + \sum \left(\frac{ax^2 + 2bxy + cy^2}{\sigma} \right)^{-s} + \cdots \\ - \sum \left(\frac{a'x^2 + 2b'xy + c'y^2}{\sigma} \right)^{-s} - \cdots \end{array} \right\},$$

wo auf der rechten Seite die den H Formen (a, b, c) der ersten Gruppe entsprechenden Doppelsummen mit positivem Vorzeichen, und die den H' Formen (a', b', c') der zweiten Gruppe entsprechenden Doppelsummen mit negativem Vorzeichen behaftet sind.

Multiplicirt man jetzt die Gleichung mit der unendlichen Reihe

$$\sum \frac{1}{n^{2s}},$$

so erhält man links zufolge der obigen Gleichung das Resultat

$$\varkappa \sum \frac{\chi(n)}{n^s} \sum \left(\frac{D}{n} \right) \frac{\chi(n)}{n^s};$$

führt man ferner auf der rechten Seite die Multiplication wie in §. 90 aus, so verändert sich äusserlich ihre Gestalt nicht, sondern es fällt allein die frühere Bedingung III. fort, nach welcher die den Variabeln x, y beigelegten Werthe relative Primzahlen zu einander sein mussten. Man erhält daher

$$\varkappa \sum \frac{\chi(n)}{n^s} \sum \left(\frac{D}{n} \right) \frac{\chi(n)}{n^s} = \left\{ \begin{array}{l} + \sum \left(\frac{ax^2 + 2bxy + cy^2}{\sigma} \right)^{-s} + \cdots \\ - \sum \left(\frac{a'x^2 + 2b'xy + c'y^2}{\sigma} \right)^{-s} - \cdots \end{array} \right\}.$$

Setzen wir jetzt $s = 1 + \varrho$, und multipliciren wir mit ϱ, so nähert sich mit unendlich abnehmendem positiven ϱ jedes der h Producte

$$\varrho\,\Sigma\left(\frac{ax^2+2bxy+cy^2}{\sigma}\right)^{-(1+\varrho)}\cdots\varrho\,\Sigma\left(\frac{a'x^2+2b'xy+c'y^2}{\sigma}\right)^{-(1+\varrho)}\cdots$$

einem und demselben von Null verschiedenen Grenzwerth W, welcher für eine negative Determinante in §. 95, für eine positive in §. 98 bestimmt ist; mithin wird der Grenzwerth, welchem sich das Product aus ϱ und aus der rechten Seite der vorstehenden Gleichung nähert, gleich $(H-H')\,W$.

Für die beiden Fälle nun, in welchen für $\chi(n)$ entweder das Anfangsglied 1 oder das Glied $\Pi\,C'$ der Entwicklung des Productes $\Pi(1+C)$ genommen wird, ist $H=h$ und $H'=0$; und die obige Gleichung stimmt genau mit der in §. 90 überein, welche später zur Bestimmung der Classenanzahl h führte. In den übrigen $(2\tau-2)$ Fällen, d. h. also, wenn unter $\chi(n)$ irgend ein Glied des entwickelten Ausdrucks

$$\Pi\,(1+C)-1-\Pi\,C'$$

verstanden wird, nähert sich aber, wie im folgenden Paragraphen nachträglich gezeigt werden soll, jede der beiden unendlichen Reihen

$$\Sigma\,\frac{\chi(n)}{n^{1+\varrho}}\quad\text{und}\quad\Sigma\left(\frac{D}{n}\right)\frac{\chi(n)}{n^{1+\varrho}}$$

mit unendlich abnehmendem ϱ einem *endlichen* Grenzwerth, und folglich das Product

$$\varrho\,\varkappa\,\Sigma\,\frac{\chi(n)}{n^{1+\varrho}}\cdot\Sigma\left(\frac{D}{n}\right)\frac{\chi(n)}{n^{1+\varrho}}$$

dem Grenzwerth Null. Vergleicht man dies mit dem oben gefundenen Grenzwerth $(H-H')\,W$, wo W eine von Null verschiedene Grösse war, so ergiebt sich

$$H-H'=0,$$

d. h. jedem dieser $(2\tau-2)$ Fälle entspricht eine Eintheilung aller h Formen des Systems S in zwei Gruppen, deren jede eine gleiche Anzahl $H=H'=\frac{1}{2}h$ Formen enthält.

Zufolge der obigen Bemerkung, dass die g_r Formen des Systems S, welche einem und demselben Geschlecht G_r angehören, bei jeder einzelnen Specialisirung von $\chi(n)$ entweder alle in die erste, oder alle in die zweite Gruppe fallen, lässt sich jede solche Gleichung von der Form $H-H'=0$, welche einem dieser $(2\tau-2)$ Fälle entspricht, in folgender Weise aufschreiben

$$g_1 \pm g_2 \pm g_3 \pm \cdots \pm g_\tau = 0, \qquad (g)$$

wo die Anzahl g_1 jedesmal mit positivem, irgend eine andere Anzahl g_r aber mit positivem oder negativem Vorzeichen behaftet ist, je nachdem in diesem Fall die Formen des Geschlechts G_r derselben Gruppe angehören, wie die Formen des Geschlechts G_1, oder nicht, d. h. je nachdem die Werthe, welche $\chi(n)$ in dem Geschlecht G_1 und in dem Geschlecht G_r erhält, gleich oder entgegengesetzt sind. Ist Δ der Ueberschuss der Anzahl der Fälle, in welchen das Erstere eintritt, über die Anzahl der übrigen, so wird, wenn man alle Gleichungen (g) addirt, die den $(2\tau - 2)$ verschiedenen Fällen entsprechen, der Coefficient von g_1 gleich $(2\tau - 2)$, und der von g_r gleich Δ werden. Um nun diesen Ueberschuss Δ zu bestimmen, bezeichnen wir mit γ_1 und γ_r die bestimmten Werthe ± 1, welche irgend einer der λ Charaktere C resp. in dem Geschlecht G_1 und G_r annimmt, und unter diesen mit γ_1' und γ_r' diejenigen Werthe, welche den Charakteren C' entsprechen; man überzeugt sich dann leicht, dass

$$\Delta = \Pi\,(1 + \gamma_1\gamma_r) - 1 - \Pi\,\gamma_1'\gamma_r'$$

ist; denn wenn wir das erste, aus λ Factoren von der Form $(1 + \gamma_1\gamma_r)$ bestehende, Product rechter Hand entwickeln und die daraus entstehenden beiden Glieder 1 und $\Pi\,\gamma_1'\gamma_r'$ gegen die beiden andern Glieder fortheben, so bleiben $2^\lambda - 2 = 2\tau - 2$ Glieder zurück, deren jedes einem bestimmten Gliede des entwickelten Ausdrucks

$$\Pi\,(1 + C) - 1 - \Pi\,C',$$

d. h. einer bestimmten Specialisirung von $\chi(n)$ entspricht, und zwar wird ein solches Glied $= +1$ oder $= -1$ werden, je nachdem die beiden Werthe, welche das correspondirende $\chi(n)$ im Geschlecht G_1 und im Geschlecht G_r annimmt, gleich oder entgegengesetzt ausfallen; die algebraische Summe aller dieser Glieder ist also in der That gleich dem Ueberschuss Δ, was zu beweisen war. Da nun die beiden Geschlechter G_1 und G_r verschieden sind, so ist mindestens einer der λ Factoren $(1 + \gamma_1\gamma_r)$ gleich Null, und da ausserdem $\Pi\,\gamma_1' = 1$, $\Pi\,\gamma_r' = 1$ und folglich auch $\Pi\,\gamma_1'\gamma_r' = 1$ ist, so erhalten wir $\Delta = -2$. Da dieser Ueberschuss Δ nun für alle von G_1 verschiedenen Geschlechter gleich gross ist, so erhalten wir durch Addition sämmtlicher $(2\tau - 2)$ Gleichungen (g) das Resultat

$$(2\tau - 2)\,g_1 - 2\,(g_2 + g_3 + \cdots + g_\tau) = 0,$$

und da ausserdem

$$g_1 + g_2 + g_3 + \cdots + g_\tau = h$$

ist, so folgt

$$2\tau g_1 - 2h = 0, \quad \text{also} \quad g_1 = \frac{h}{\tau} = \frac{h}{2^{\lambda-1}}.$$

Da endlich für jedes andere Geschlecht G_2, $G_3 \ldots G_\tau$ die Untersuchung ebenso geführt werden kann, wie für das Geschlecht G_1, so erhalten wir als Endresultat den Satz*):

Die Anzahl der wirklich existirenden Geschlechter ist gleich $2^{\lambda-1}$, *und alle diese Geschlechter enthalten gleich viele Formenclassen.*

§. 126.

Zur Vervollständigung des vorstehenden Beweises haben wir nun noch zu zeigen, dass für jede der $2\tau - 2$ Specialisirungen von $\chi(n)$, welche den Gliedern des obigen entwickelten Ausdrucks entsprechen, jede der beiden unendlichen Reihen

$$\Sigma \frac{\chi(n)}{n^{1+\varrho}}, \quad \Sigma \left(\frac{D}{n}\right) \frac{\chi(n)}{n^{1+\varrho}}$$

mit unendlich abnehmendem positiven ϱ sich einem endlichen Grenzwerth nähert. Dies kann mit Rücksicht auf frühere Untersuchungen (§. 101) in folgender Weise geschehen.

Jede der beiden in Rede stehenden Summen ist von der Form

$$\Sigma \frac{\alpha_n}{n^s} = \Sigma\, \theta^{1/2(n-1)}\, \eta^{1/8(n^2-1)} \left(\frac{n}{L}\right) \frac{1}{n^s},$$

*) *Gauss: D. A.* artt. 252, 261, 287. — Mit Hülfe des Satzes über die arithmetische Progression (Supplement VI.) lässt sich der obige Satz sehr kurz beweisen. Da nämlich alle Zahlen n, für welche jeder der λ Charaktere C einen vorgeschriebenen Werth $+1$ besitzt, in gewissen arithmetischen Reihen enthalten sind, deren Differenz $4D$ ist, während ihre Anfangsglieder relative Primzahlen zu $4D$ sind (vergl. §. 52), so existiren unter diesen Zahlen n auch *Primzahlen* p; genügen nun die für die Charaktere C vorgeschriebenen Werthe $+1$ der Bedingung $\Pi C' = +1$, so ist D *quadratischer Rest von* p, und folglich existirt eine (positive) ursprüngliche Form erster Art, deren erster Coefficient $= p$ ist, welche mithin den vorgeschriebenen Total-Charakter besitzt.

wo $\theta^2 = 1$, $\eta^2 = 1$, und L irgend ein ungerader Divisor von D ist; da quadratische Factoren im Nenner eines Jacobi'schen Symbols fortgelassen werden dürfen, so können wir annehmen, dass L durch keine Quadratzahl (ausser 1) theilbar ist. Ferner ist jedenfalls nicht gleichzeitig $\theta = +1$, $\eta = +1$, $L = 1$; denn sonst wäre entweder $\chi(n) = 1$, oder $\chi(n) = \Pi C'$, gegen unsere Voraussetzung.

Bezeichnen wir mit LL' das Product aus allen von einander verschiedenen in D aufgehenden ungeraden Primzahlen, so ist das System der Zahlen n identisch mit dem System aller positiven ganzen Zahlen, welche relative Primzahlen zu $8LL'$ sind; wir betrachten zunächst nur die ersten $\varphi(8LL')$ Zahlen n, d. h. diejenigen Zahlen n, welche kleiner als $8LL'$ sind, und zeigen, dass die Summe der entsprechenden Werthe von α_n gleich Null ist. Zu diesem Zwecke bezeichnen wir mit a irgend eine der vier Zahlen 1, 3, 5, 7; mit b irgend eine der $\varphi(L)$ Zahlen, welche relative Primzahlen zu L und nicht grösser als L sind; endlich mit b' irgend eine der $\varphi(L')$ Zahlen, welche relative Primzahlen zu L' und nicht grösser als L' sind. Es wird dann (nach §. 25) durch die drei Congruenzen

$$n \equiv a \pmod 8, \quad n \equiv b \pmod L, \quad n \equiv b' \pmod{L'}$$

eine und nur eine Zahl n bestimmt, welche relative Primzahl zu $8LL'$ und zugleich kleiner als $8LL'$ ist; und wenn jede der drei Zahlen a, b, b' unabhängig von den anderen alle ihr zukommenden Werthe durchläuft, so werden auf diese Weise auch alle $\varphi(8LL')$ Zahlen n erzeugt, die relative Primzahlen zu $8LL'$ und kleiner als $8LL'$ sind. Da nun jedesmal

$$\theta^{\frac{1}{2}(a-1)}\,\eta^{\frac{1}{8}(a^2-1)} = \theta^{\frac{1}{2}(n-1)}\,\eta^{\frac{1}{8}(n^2-1)}, \left(\frac{n}{L}\right) = \left(\frac{b}{L}\right)$$

ist, so wird die über diese Werthe von n ausgedehnte Summe

$$\Sigma\,\alpha_n = \varphi(L') \cdot \Sigma\,\theta^{\frac{1}{2}(a-1)}\,\eta^{\frac{1}{8}(a^2-1)} \cdot \Sigma\left(\frac{b}{L}\right);$$

nun ist aber (nach §. 52, I.)

$$\Sigma\left(\frac{b}{L}\right) = 0,$$

ausgenommen, wenn $L = 1$ ist; ausserdem findet man leicht, dass auch

$$\Sigma\,\theta^{\frac{1}{2}(a-1)}\,\eta^{\frac{1}{8}(a^2-1)} = 0$$

ist, ausgenommen, wenn $\theta = \eta = +1$ ist. Da nun, wie schon oben bemerkt ist, diese beiden Ausnahmefälle jedenfalls nicht gleichzeitig eintreten, so ist

$$\Sigma\, \alpha_n = 0,$$

wo das Summenzeichen sich auf die angegebenen Werthe von n bezieht.

Da ferner, sobald $n' \equiv n \pmod{8LL'}$, auch $\alpha_{n'} = \alpha_n$ ist, so wird immer

$$\Sigma\, \alpha_n = 0$$

sein, wenn die Summation auf beliebige $\varphi(8LL')$ auf einander folgende, also nach dem Modul $8LL'$ incongruente Werthe von n ausgedehnt wird. Und hieraus folgt unmittelbar, dass die Summe aller Werthe von α_n, die beliebig vielen auf einander folgenden Werthen von n entsprechen (von $n = 1$ an gerechnet) stets unterhalb einer endlichen angebbaren Grenze bleibt. Nach einer frühern Untersuchung (§. 101) ist daher die Reihe

$$\Sigma\, \frac{\alpha_n}{n^s},$$

wenn ihre Glieder nach der Grösse der Nenner geordnet werden, eine für jeden positiven Werth von s endliche und stetige Function von s; also nähert sich auch jede der beiden obigen Reihen mit unendlich abnehmendem positiven ϱ einem endlichen Grenzwerth, was zu beweisen war.

V. Theorie der Potenzreste für zusammengesetzte Moduli.

§. 127.

Es ist in §. 28 gezeigt, dass wenn die Zahl a relative Primzahl gegen den Modul k ist, stets positive ganze Exponenten n von der Beschaffenheit existiren, dass $a^n \equiv 1 \pmod{k}$ ist; diese Exponenten n sind die sämmtlichen Vielfachen des kleinsten unter ihnen; bezeichnet man diesen mit δ, so sagt man, die Zahl *a gehöre* zum Exponenten δ; und die δ Zahlen

$$1,\ a,\ a^2 \ldots a^{\delta-1} \qquad (A)$$

sind sämmtlich incongruent. Mit Hülfe des verallgemeinerten Fermat'schen Satzes ist dort ebenfalls gezeigt, dass δ immer ein Divisor von $\varphi(k)$ ist; dies Resultat lässt sich aber auch ohne Hülfe des Fermat'schen Satzes ableiten durch eine eigenthümliche Methode, welche sehr häufig zum Nachweise der Theilbarkeit einer Zahl durch eine andere gebraucht werden kann. In unserm Falle gestaltet dieselbe sich folgendermaassen.

Ist a' irgend eine relative Primzahl zu k, so sind (nach §. 18) die δ Zahlen

$$a',\ a'a,\ a'a^2 \ldots a'a^{\delta-1} \qquad (A')$$

sämmtlich incongruent; dasselbe gilt von den δ Zahlen

$$a'',\ a''a,\ a''a^2 \ldots a''a^{\delta-1} \qquad (A'')$$

sobald a'' ebenfalls relative Primzahl zu k ist. Jeder solche Complex, wie A' oder A'', enthält δ unter einander incongruente Zahlen, die sämmtlich relative Primzahlen gegen k sind und also als

Repräsentanten von δ Zahl-Classen in Bezug auf den Modul k angesehen werden können. Gesetzt nun, es findet sich eine und dieselbe Zahlclasse in jedem der beiden Complexe A' und A'' vertreten, so giebt es zwei Exponenten μ', μ'' von der Beschaffenheit, dass

$$a' \cdot a^{\mu'} \equiv a'' \cdot a^{\mu''} \pmod{k}$$

ist; nehmen wir an, was der Symmetrie wegen erlaubt ist, dass $\mu'' \geqq \mu'$, so erhält man durch Division mit $a^{\mu'}$ die Congruenz

$$a' \equiv a'' \cdot a^{\mu''-\mu'} \pmod{k};$$

und hieraus folgt sogleich, dass *jede* in A' enthaltene Zahl $a' \cdot a^m$ auch einer Zahl von der Form $a'' \cdot a^n$, d. h. einer in A'' enthaltenen Zahl congruent ist. Wir können hieraus schliessen, dass entweder zwei solche Complexe A', A'' dieselben δ Zahlclassen enthalten, oder dass keine einzige Classe in beiden gleichzeitig vertreten ist.

Bildet man nun der Reihe nach alle solche aus δ Zahlclassen bestehenden Complexe von der Form A', A'' ..., und zwar nur solche, welche von einander verschieden sind, so muss endlich jede der $\varphi(k)$ Zahlclassen, welche relative Primzahlen zu k enthalten, in einem dieser Complexe, und auch nur in einem, vertreten sein; ist daher ε die Anzahl dieser von einander verschiedenen Complexe, so muss $\varphi(k) = \varepsilon\delta$, also $\varphi(k)$ theilbar durch δ sein, was zu beweisen war.

Hieraus ergiebt sich nun der Fermat'sche Satz als Folgerung; denn erhebt man die Congruenz

$$a^{\delta} \equiv 1 \pmod{k}$$

zur εten Potenz, so erhält man

$$a^{\varphi(k)} \equiv 1 \pmod{k}.$$

§. 128.

Für den Fall, dass der Modul k eine Primzahl p ist, wurde ferner in §. 29 bewiesen, dass zu jedem Divisor δ von $\varphi(p) = p-1$ genau $\varphi(\delta)$ Zahlen gehören, die nach dem Modul p incongruent sind; und in §. 30 sind die Eigenschaften der sogenannten primi-

tiven Wurzeln von p betrachtet, d. h. derjenigen $\varphi(p-1)$ incongruenten Zahlen g, welche zum Exponenten $p-1$ selbst gehören. Wir wollen nun untersuchen, ob ähnliche Gesetze auch für zusammengesetzte Moduln gelten.

Zunächst beschränken wir uns auf den Fall, in welchem der Modul k eine *Potenz von einer ungeraden Primzahl* p ist, und wir werden der Analogie nach unter einer *primitiven Wurzel* von k jede Zahl g verstehen, welche zum Exponenten $\varphi(k)$ gehört. Dem Beweise der wirklichen Existenz solcher primitiven Wurzeln schicken wir folgenden Hülfssatz voraus:

Ist h irgend eine ganze Zahl und $\pi \geqq 1$ eine positive ganze Zahl, so ist stets

$$(1+hp^{\pi})^{p} \equiv 1 + hp^{\pi+1} \pmod{p^{\pi+2}}.$$

Man überzeugt sich hiervon leicht durch die Entwicklung der linken Seite nach dem binomischen Satze; man findet nämlich zunächst, indem man sich auf die drei ersten Glieder beschränkt,

$$(1+hp^{\pi})^{p} \equiv 1 + hp^{\pi+1} + \tfrac{1}{2}(p-1)h^{2}p^{2\pi+1} \pmod{p^{3\pi}},$$

und hieraus ergiebt sich die obige Congruenz, wenn man bedenkt, dass p ungerade, also $\frac{1}{2}(p-1)$ eine ganze Zahl, und ferner, dass sowohl $p^{2\pi+1}$ als auch $p^{3\pi}$ durch $p^{\pi+2}$ theilbar ist.

Nach dieser Vorbemerkung gehen wir an unsere Untersuchung und nehmen zunächst einmal an, es existire für den Modul $p^{\pi+1}$, wo $\pi \geqq 1$ ist, wirklich eine primitive Wurzel g; dann liegt es nahe zu fragen: zu welchem Exponenten gehört eine solche Zahl g in Bezug auf den Modul p^{π}? Es sei δ dieser Exponent, also

$$g^{\delta} = 1 + hp^{\pi},$$

so erhält man mit Hülfe des soeben bewiesenen Satzes

$$g^{\delta p} \equiv 1 \pmod{p^{\pi+1}};$$

da nun g primitive Wurzel von $p^{\pi+1}$ ist, so muss δp durch $\varphi(p^{\pi+1}) = (p-1)p^{\pi}$, und folglich δ durch $(p-1)p^{\pi-1}$ theilbar sein; andererseits muss aber, da g zum Exponenten δ in Bezug auf den Modul p^{π} gehört, nothwendig $\varphi(p^{\pi}) = (p-1)p^{\pi-1}$ durch δ theilbar sein; mithin ist $\delta = \varphi(p^{\pi})$, d. h. g ist auch primitive Wurzel von p^{π}. Zugleich leuchtet ein, dass die in der Gleichung

$$g^{(p-1)p^{\pi-1}} = 1 + hp^{\pi}$$

vorkommende Zahl h nicht durch p theilbar sein kann; denn sonst wäre

$$g^{(p-1)p^{\pi-1}} \equiv 1 \pmod{p^{\pi+1}},$$

also g keine primitive Wurzel von $p^{\pi+1}$.

Setzt man diese Schlüsse weiter fort, so erhält man zunächst das Resultat:

Jede primitive Wurzel g von einer höhern Potenz einer ungeraden Primzahl p ist nothwendig eine primitive Wurzel der Zahl p selbst, und zwar von der Beschaffenheit, dass $g^{p-1}-1$ nicht durch p^2 theilbar ist.

Wir wollen nun umgekehrt annehmen, es sei g eine primitive Wurzel von p^π, und zwar von der Beschaffenheit, dass die in der Gleichung

$$g^{(p-1)p^{\pi-1}} = 1 + hp^\pi$$

vorkommende Zahl h nicht durch p theilbar ist; und wir fragen jetzt: zu welchem Exponenten gehört diese Zahl g in Bezug auf den Modul $p^{\pi+1}$? Ist δ dieser Exponent, also

$$g^\delta \equiv 1 \pmod{p^{\pi+1}},$$

so ist auch

$$g^\delta \equiv 1 \pmod{p^\pi},$$

und folglich δ theilbar durch $\varphi(p^\pi)$; da aber andererseits δ ein Divisor von $\varphi(p^{\pi+1}) = p\varphi(p^\pi)$ sein muss, so ist δ entweder $= \varphi(p^\pi)$, oder $= \varphi(p^{\pi+1})$; das Erstere ist aber nicht der Fall, weil unserer Voraussetzung zufolge die Zahl h nicht durch p theilbar ist; also ist $\delta = \varphi(p^{\pi+1})$, d. h. die Zahl g ist primitive Wurzel von $p^{\pi+1}$. Zugleich leuchtet aus der Congruenz

$$g^{(p-1)p^\pi} = (1 + hp^\pi)^p \equiv 1 + hp^{\pi+1} \pmod{p^{\pi+2}}$$

ein, dass die in der Gleichung

$$g^{(p-1)p^\pi} = 1 + h'p^{\pi+1}$$

vorkommende Zahl h' nicht durch p theilbar ist.

Durch Fortsetzung dieser Schlussweise erhalten wir das zweite Resultat:

Jede primitive Wurzel g einer ungeraden Primzahl p, für welche die Differenz $g^{p-1}-1$ nicht durch p^2 theilbar ist, ist auch eine primitive Wurzel aller höheren Potenzen von p.

Um also die Existenz von primitiven Wurzeln g für höhere Potenzen von p nachzuweisen, und um alle diese Zahlen g zu finden, haben wir nur noch zu zeigen, dass in der That primitive Wurzeln g von p existiren, für welche $g^{p-1} - 1$, oder, was dasselbe sagt, für welche $g^p - g$ nicht durch p^2 theilbar ist. Dies geschieht leicht auf folgende Weise. Ist f irgend eine primitive Wurzel von p, so sind alle in der Form

$$g = f + px$$

enthaltenen Zahlen g ebenfalls primitive Wurzeln von p; dann ist nach dem binomischen Satze

$$g^p \equiv f^p \pmod{p^2};$$

setzen wir daher

$$f^p \equiv f + f'p \pmod{p^2},$$

so wird

$$g^p - g \equiv p(f' - x) \pmod{p^2},$$

und folglich ist $g = f + px$ jedesmal eine primitive Wurzel aller Potenzen von p, ausgenommen, wenn $x \equiv f' \pmod{p}$, also

$$g \equiv f^p \pmod{p^2}$$

ist. Da nun $\varphi(p-1)$ nach dem Modul p incongruente Zahlen f existiren, und aus jeder Zahl f genau $(p-1)$ in Bezug auf den Modul p^2 incongruente Zahlen $g = f + px$ von der Beschaffenheit abgeleitet werden können, dass $g^{p-1} - 1$ nicht durch p^2 theilbar wird, so erhalten wir das Resultat:

Die sämmtlichen primitiven Wurzeln von höheren Potenzen einer ungeraden Primzahl p sind die sämmtlichen Individuen von $(p-1)\,\varphi(p-1)$ verschiedenen Zahlclassen in Bezug auf den Modul p^2.

Beispiel: Sämmtliche primitive Wurzeln der Primzahl $p = 7$ sind in den beiden Reihen $7x + 3$, $7x + 5$ enthalten; da nun

$$3^7 \equiv 31, \quad 5^7 \equiv 19 \pmod{49}$$

ist, so sind alle in den arithmetischen Reihen $7x + 3$, $7x + 5$ enthaltenen Zahlen, mit Ausnahme derer, welche $\equiv 31$ oder $\equiv 19 \pmod{49}$ sind, auch primitive Wurzeln von allen höheren Potenzen von 7.

§. 129.

Nachdem im Vorhergehenden die Existenz von primitiven Wurzeln g für jeden Modul p^π nachgewiesen ist, der eine Potenz einer ungeraden Primzahl p ist, kann man leicht die übrigen elementaren Fragen über die Potenzreste beantworten. Setzt man zur Abkürzung

$$\varphi(p^\pi) = c,$$

so sind die Potenzen

$$g^0,\ g^1,\ g^2 \ldots g^{c-1} \pmod{p^\pi}$$

sämmtlich incongruent, und bilden daher ein vollständiges System incongruenter Zahlen, mit Ausschluss der durch p theilbaren Zahlen. Ist daher n irgend eine durch p nicht theilbare Zahl, so existiren stets unendlich viele Exponenten γ, die aber nach dem Modul c sämmtlich einander congruent sind, von der Beschaffenheit, dass

$$n \equiv g^\gamma \pmod{p^\pi};$$

man nennt dann γ den *Index der Zahl n für die Basis g*, und drückt dies in Zeichen so aus

$$\text{Ind. } n \equiv \gamma \pmod{c};$$

durchläuft γ ein vollständiges Restsystem in Bezug auf den Modul c, so durchläuft n ein vollständiges System von Zahlen, die relative Primzahlen zu p^π und unter einander nach dem Modul p^π incongruent sind. Für die Rechnung mit diesen Indices gelten dieselben Gesetze, wie die (in §. 30 angegebenen) für den Fall $\pi = 1$. Wir heben hier besonders hervor, dass

$$\text{Ind. } (1) \equiv 0,\ \text{Ind. } (-1) \equiv \tfrac{1}{2}c \pmod{c},$$

und ferner, dass n quadratischer Rest oder Nichtrest von p^π ist, je nachdem Ind. n gerade oder ungerade ist.

Aus dem Index einer Zahl n lässt sich leicht der Exponent t bestimmen, zu welchem n in Bezug auf den Modul p^π gehört; aus

$$n \equiv g^{\text{Ind. } n} \pmod{p^\pi}$$

folgt nämlich

$$n^t \equiv g^{t\,\mathrm{Ind}.n} \pmod{p^\pi};$$

soll also $n^t \equiv 1$ sein, so muss t Ind. n durch c theilbar, und folglich t ein Multiplum von $c : \delta$ sein, wo δ den grössten gemeinschaftlichen Divisor von c und Ind. n bedeutet; die kleinste aller dieser Zahlen t, d. h. der Exponent, zu welchem n gehört, ist daher $= c : \delta$.

Hieraus folgt, dass n stets und nur dann eine primitive Wurzel von p^π ist, wenn Ind. n relative Primzahl zu c ist; die Anzahl aller nach dem Modul p^π incongruenten primitiven Wurzeln von p^π ist daher gleich der Anzahl derjenigen der Zahlen

$$0,\ 1,\ 2 \ldots c-1,$$

welche relative Primzahlen zu c sind, also gleich $\varphi(c) = \varphi\varphi(p^\pi)$. Dasselbe Resultat ist aber auch eine unmittelbare Folge aus dem Schlusssatze des vorigen Paragraphen.

§. 130.

Die Primzahl 2 verhält sich anders als die ungeraden Primzahlen, welche bisher ausschliesslich betrachtet wurden.

Für den Modul 2 kann jede ungerade Zahl als primitive Wurzel angesehen werden.

Für den Modul $2^2 = 4$ ist $3 \equiv -1$ eine primitive Wurzel; zu jeder ungeraden Zahl n giebt es einen entsprechenden Exponenten α von der Beschaffenheit, dass

$$n \equiv (-1)^\alpha \pmod{4}$$

ist; und zwar ist $\alpha \equiv 0 \pmod{2}$ oder $\equiv 1 \pmod{2}$, je nachdem $n \equiv 1$ oder $\equiv 3 \pmod{4}$ ist.

Bis hierher findet also noch völlige Analogie mit den ungeraden Primzahlen Statt; sobald aber ein Modul 2^λ betrachtet wird, in welchem der Exponent $\lambda \geqq 3$ ist, hört dieselbe auf. Es lässt sich nämlich zeigen, dass, wenn n irgend eine ungerade Zahl bedeutet, immer schon

$$n^{\frac{1}{2}\varphi(2^\lambda)} = n^{2^{\lambda-2}} \equiv 1 \pmod{2^\lambda}$$

ist. In der That ist dieser Satz richtig für $\lambda = 3$; denn das Quadrat jeder ungeraden Zahl n ist $\equiv 1 \pmod{8}$. Nehmen wir

ferner an, der Satz sei für einen beliebigen Exponenten $\lambda \geqq 3$ schon bewiesen, es sei also

$$n^{2^{\lambda-2}} = 1 + h\,2^{\lambda},$$

so folgt hieraus durch Quadriren

$$n^{2^{\lambda-1}} = 1 + h\,2^{\lambda+1} + h^2 2^{2\lambda} \equiv 1 \pmod{2^{\lambda+1}},$$

d. h. der Satz gilt auch für den nächstfolgenden Exponenten $\lambda + 1$. Er gilt mithin allgemein, da er für $\lambda = 3$ gilt.

Es fragt sich nun, ob es in diesen Fällen wenigstens Zahlen giebt, die zu dem Exponenten $\frac{1}{2}\varphi(2^{\lambda}) = 2^{\lambda-2}$ gehören; man überzeugt sich leicht, dass die Zahl 5 diese Eigenschaft für jeden Modul $2^{\lambda} \geqq 8$ besitzt. Es ist nämlich

$$5 \equiv 1 + 4 \pmod{8}$$
$$5^2 \equiv 1 + 8 \pmod{16}$$
$$5^4 \equiv 1 + 16 \pmod{32}$$
$$5^8 \equiv 1 + 32 \pmod{64}$$

allgemein

$$5^{2^{\lambda-3}} \equiv 1 + 2^{\lambda-1} \pmod{2^{\lambda}},$$

also

$$5^{2^{\lambda-3}} \text{ niemals} \equiv 1 \pmod{2^{\lambda}},$$

woraus unmittelbar folgt, dass der Exponent, zu welchem die Zahl 5 nach dem Modul 2^{λ} gehört, kein Divisor von $2^{\lambda-3}$ sein kann, und also, da er doch Divisor von $2^{\lambda-2}$ sein muss, nothwendig $= 2^{\lambda-2}$ ist.

Hieraus ergiebt sich nun, wenn man zur Abkürzung

$$\tfrac{1}{2}\varphi(2^{\lambda}) = 2^{\lambda-2} = b$$

setzt, dass die b Zahlen

$$5^0,\ 5^1,\ 5^2 \ldots 5^{b-1}$$

sämmtlich nach dem Modul 2^{λ} incongruent sind; dasselbe gilt von den Zahlen

$$-5^0,\ -5^1,\ -5^2 \ldots -5^{b-1}$$

da ferner die erstern sämmtlich $\equiv 1 \pmod 4$, die letztern sämmtlich $\equiv 3 \pmod 4$ sind, so bilden sie zusammengenommen ein System von $\varphi(2^{\lambda})$ nach dem Modul 2^{λ} incongruenten ungeraden Zahlen. Ist daher n irgend eine ungerade Zahl, so kann man stets

$$n \equiv (-1)^{\alpha} 5^{\beta} \pmod{2^{\lambda}}$$

setzen, wo α nach dem Modul 2, und β nach dem Modul b vollständig bestimmt ist. Durchläuft α ein vollständiges Restsystem in Bezug auf den Modul 2, und β unabhängig von α ein vollständiges Restsystem in Bezug auf den Modul b, so durchläuft n ein vollständiges System von Zahlen, die in Bezug auf den Modul 2^{λ} incongruent und relative Primzahlen zu 2^{λ}, d. h. ungerade sind. Diese beiden Zahlen α und β kann man die *Indices* der Zahl n nennen; sie befolgen ganz ähnliche Gesetze, wie die Indices für die früher betrachteten Moduli. Wir heben noch besonders hervor, dass $n \equiv \pm 1$ oder $\equiv \pm 3 \pmod 8$ ist, je nachdem β gerade oder ungerade.

Es verdient bemerkt zu werden, dass die vorstehende Form, in welche jede ungerade Zahl n gebracht werden kann, auch noch für den Fall $\lambda = 2$ gilt; die Anzahl b der Werthe von β reducirt sich nämlich auf 1, und da $5 \equiv 1 \pmod 4$, so geht die obige Form in die frühere $n \equiv (-1)^{\alpha} \pmod 4$ über. Für eine spätere Untersuchung ist es sogar zweckmässig, dieselbe Form der Darstellung aller relativen Primzahlen zu einem Modul von der Form 2^{λ} auf die Fälle $\lambda = 0$ und $\lambda = 1$ auszudehnen; da in denselben nur eine einzige Zahlclasse darzustellen ist, so wird man α und β auch nur einen einzigen Werth beizulegen haben; setzen wir daher $a = b = 1$, wenn $\lambda = 0$ oder $\lambda = 1$ ist, in allen anderen Fällen ($\lambda \geqq 2$) aber $a = 2$, $b = \frac{1}{2}\varphi(2^{\lambda})$, so können wir sagen, dass der Ausdruck

$$n \equiv (-1)^{\alpha} 5^{\beta} \pmod{2^{\lambda}}$$

alle incongruenten relativen Primzahlen zum Modul durchläuft, wenn α und β resp. vollständige Restsysteme in Bezug auf a und b durchlaufen.

§. 131.

Es sei nun der Modul eine beliebige zusammengesetzte Zahl

$$k = 2^{\lambda} p^{\pi} p'^{\pi'} \ldots,$$

wo p, p' von einander verschiedene ungerade Primzahlen, und λ, π, π' . . . ganze positive Exponenten bedeuten, deren erster, λ,

auch $= 0$ sein kann. Ist n irgend eine relative Primzahl zu k, so kann man stets

$$n \equiv (-1)^{\alpha} 5^{\beta} \pmod{2^{\lambda}}$$
$$n \equiv g^{\gamma} \pmod{p^{\pi}}$$
$$n \equiv g'^{\gamma'} \pmod{p'^{\pi'}}$$
$$\ldots\ldots\ldots\ldots$$

setzen, wo $g, g' \ldots$ primitive Wurzeln resp. von $p^2, p'^2 \ldots$ bedeuten. Geben wir den Zahlen a, b die im vorigen Paragraphen festgesetzte Bedeutung und setzen wir zur Abkürzung

$$\varphi(p^{\pi}) = c, \quad \varphi(p'^{\pi'}) = c' \ldots,$$

so sind die Exponenten oder Indices

$$\alpha, \ \beta, \ \gamma, \ \gamma' \ldots$$

vollständig bestimmt in Bezug auf die entsprechenden Moduli

$$a, \ b, \ c, \ c' \ldots,$$

und umgekehrt entspricht jedem solchen Systeme von Indices (nach §. 25) eine bestimmte Classe von Zahlen n nach dem Modul k, die relative Primzahlen zu k sind. Durchlaufen die Indices $\alpha, \beta, \gamma, \gamma' \ldots$ unabhängig von einander ihre $a, b, c, c' \ldots$ Werthe, so durchläuft n sämmtliche

$$abcc' \ldots = \varphi(k)$$

Zahlclassen in Bezug auf den Modul k, welche relative Primzahlen zu k enthalten.

Sind die Indices $\alpha, \beta, \gamma, \gamma' \ldots$ einer Zahl n bekannt, so ist es leicht, den Exponenten δ zu bestimmen, zu welchem die Zahl n gehört; denn offenbar ist δ das kleinste gemeinschaftliche Multiplum aller derjenigen Exponenten, zu welchen die Zahl n in Bezug auf die einzelnen Moduli $2^{\lambda}, p^{\pi}, p'^{\pi'} \ldots$ gehört. Dieser Exponent δ ist daher immer ein Divisor von dem kleinsten gemeinschaftlichen Vielfachen μ der Zahlen $a, b, c, c' \ldots$ Es können daher primitive Wurzeln von k, d. h. Zahlen, die zum Exponenten $\varphi(k)$ gehören, nur dann existiren, wenn $\mu = \varphi(k)$ ist; man überzeugt sich leicht, dass dies nur dann der Fall ist, wenn der Modul $k = 1$, oder $= 2$, oder $= 4$, oder eine Potenz einer ungeraden Primzahl, oder das Doppelte einer solchen Potenz ist; und umgekehrt leuchtet ein, dass in diesen Fällen immer primitive Wurzeln existiren.

Da ferner die Möglichkeit einer binomischen Congruenz von der Form

$$x^m \equiv n \pmod{k}$$

und die Anzahl ihrer Wurzeln nur von der Möglichkeit derselben Congruenz in Bezug auf die einzelnen Moduli 2^λ, p^π, $p'^{\pi'}$ ... abhängt (nach §. 37), so überzeugt man sich leicht, dass zur Beurtheilung dieser Frage und zur Auffindung der Wurzeln der Congruenz die Kenntniss der Indices der Zahl n vollständig ausreicht. Die wirkliche Ausführung dieser Untersuchung unterdrücken wir hier, weil sie sich ganz ebenso gestaltet wie in §. 31. Der Fall $m = 2$ würde auf diese Weise behandelt auf das in §. 37 gewonnene Resultat zurückführen. Ebenso leicht ist es, den verallgemeinerten Wilson'schen Satz (§. 38) von Neuem zu beweisen.

VI. Beweis des Satzes, dass jede unbegrenzte arithmetische Progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftlichen Factor sind, unendlich viele Primzahlen enthält.

§. 132.

Der allgemeine Beweis dieses Satzes*) stützt sich auf die Betrachtung einer Classe von unendlichen Reihen von der Form

$$L = \Sigma\, \psi(n),$$

wo der Buchstabe n alle ganzen positiven Zahlen durchlaufen muss, und die reelle oder complexe Function $\psi(n)$ der Bedingung

$$\psi(n)\,\psi(n') = \psi(nn')$$

genügt. Hieraus folgt für $n = n' = 1$, dass $\psi(1) = 1$ oder $= 0$ ist; da aber im letztern Fall $\psi(n) = \psi(1)\,\psi(n)$ für alle Werthe von n verschwinden würde, so nehmen wir immer an, dass $\psi(1) = 1$ ist. Wir nehmen ferner an, die Function $\psi(n)$ sei so beschaffen, dass die Summe der analytischen Moduln aller Werthe $\psi(n)$ *endlich* ist, woraus folgt, dass die Reihe L einen von der Anordnung ihrer Glieder unabhängingen endlichen Werth besitzt. Man überzeugt sich dann leicht von der Richtigkeit der folgenden Gleichung

$$\Pi \frac{1}{1 - \psi(q)} = \Sigma\, \psi(n), \qquad (I)$$

*) *Dirichlet*: Abhandlungen der Berliner Akademie aus dem Jahre 1837.

wo das Productzeichen sich auf alle, in beliebiger Ordnung auf einander folgenden, Primzahlen q bezieht*).

Zunächst leuchtet ein, da die Reihe L die Glieder

$$\psi(1) = 1, \quad \psi(q) = z, \quad \psi(q^2) = z^2 \ldots$$

enthält, und die Summe derselben für sich einen endlichen Werth hat, dass der Modulus von $\psi(q) < 1$, und folglich

$$\frac{1}{1-\psi(q)} = 1 + \psi(q) + \psi(q^2) + \cdots$$

ist. Sind ferner $q_1, q_2, q_3 \ldots$ die sämmtlichen Primzahlen q, wie sie in dem Producte linker Hand aufeinander folgen, so wird das Product Q der ersten m Factoren

$$\frac{1}{1-\psi(q_1)}, \quad \frac{1}{1-\psi(q_2)} \cdots \frac{1}{1-\psi(q_m)},$$

wenn man jeden derselben nach der vorstehenden Gleichung in eine unendliche Reihe entwickelt und die Multiplication ausführt, gleich $\Sigma\psi(l)$, wo die Summation über alle die ganzen positiven Zahlen l auszudehnen ist, in welchen keine andern als die Primzahlen $q_1, q_2 \ldots q_m$ aufgehen. Ist daher h irgend eine positive ganze Zahl, und nimmt man m so gross, dass unter den Primzahlen $q_1, q_2 \ldots q_m$ sich alle diejenigen finden, welche $< h$ sind, so enthält $\Sigma\psi(l)$ alle Glieder der Reihe $\Sigma\psi(n)$, in welchen $n < h$ ist, und ausserdem noch unendlich viele andere, in denen $n > h$ ist. Mithin unterscheidet sich das Product Q von der Summe $\Sigma\psi(n)$ um eine Summe von der Form $\Sigma\psi(n')$, in welche aber nur noch Zahlen n' eingehen, welche $\geqq h$ sind. Da nun die Summe der Moduln aller Glieder $\psi(n)$ endlich ist, so kann man h, und also auch m so gross wählen, dass die Summe der Moduln aller Glieder $\psi(n')$, und folglich auch der Modul der Differenz $Q - \Sigma\psi(n)$ kleiner wird als jede vorher gegebene Grösse; d. h. mit unbegrenzt wachsendem m nähert sich Q dem Grenzwerth $\Sigma\psi(n)$, was zu beweisen war.

Ausser diesen Reihen von der Form $L = \Sigma\psi(n)$ haben wir noch diejenigen Reihen zu betrachten, welche durch die Entwick-

*) Unter dieser Classe von Reihen sind auch diejenigen enthalten, welche im fünften Abschnitt betrachtet sind. Vergl. §§. 124, 135. Der Werth einer solchen Function ψ ist offenbar für alle Zahlen vollständig bestimmt, sobald er für alle Primzahlen willkürlich angenommen ist. Die ältesten Untersuchungen über solche Reihen und Producte finden sich bei *Euler: Introductio in analysin infinitorum.* Cap. XV.

lung ihrer natürlichen Logarithmen entstehen. Wenn der Modulus von z ein echter Bruch ist, so ist bekanntlich

$$z + \tfrac{1}{2}z^2 + \tfrac{1}{3}z^3 + \tfrac{1}{4}z^4 + \cdots = \log \frac{1}{1-z},$$

und zwar ist der imaginäre Bestandtheil des Logarithmen rechter Hand stets zwischen den Grenzen $-\frac{1}{2}\pi i$ und $+\frac{1}{2}\pi i$ zu nehmen. Setzt man hierin $z = \psi(q)$ und für q alle Primzahlen, so erhält man zufolge der Gleichheit (I)

$$\Sigma\, \psi(q) + \tfrac{1}{2}\Sigma\, \psi(q^2) + \tfrac{1}{3}\Sigma\, \psi(q^3) + \cdots = \log L, \qquad \text{(II)}$$

und offenbar hat die aus unendlich vielen unendlichen Reihen bestehende linke Seite einen von der Anordnung der Summationen unabhängigen endlichen Werth, weil selbst die Summe der Moduln aller ihrer Glieder einen endlichen Werth besitzt. Der imaginäre Theil des Logarithmen rechter Hand ist die Summe aller imaginären Theile der Logarithmen der einzelnen Factoren, aus denen das obige unendliche Product besteht.

Wir fügen zu diesem Resultat noch einige Bemerkungen hinzu. Ist zunächst $\psi(n)$ eine reelle Function, so sind alle Factoren des unendlichen Productes positiv, also ist $\log L$ reell, und da die Reihe $\log L$ einen endlichen Werth hat, so ist L ein positiver von Null verschiedener Werth. Ist aber $\psi(n)$ imaginär, und $\psi'(n)$ der jedesmal mit $\psi(n)$ conjugirte complexe Werth, so ist auch $\psi'(n)\,\psi'(n') = \psi'(nn')$, und die über alle ganzen positiven Zahlen n ausgedehnte Summe $L' = \Sigma\,\psi'(n)$ ist die mit $L = \Sigma\,\psi(n)$ conjugirte Zahl. Zugleich wird

$$\Sigma\, \psi'(q) + \tfrac{1}{2}\Sigma\, \psi'(q^2) + \tfrac{1}{3}\Sigma\, \psi'(q^3) + \cdots = \log L',$$

und zwar ist $\log L'$ conjugirt mit $\log L$, so dass die Summe $\log L + \log L' = \log(LL')$ reell wird.

Ist endlich der Werth der Function ψ für alle in einer bestimmten Zahl k aufgehenden Primzahlen $= 0$, so ist $\psi(n)$ jedesmal $= 0$, wenn n keine relative Primzahl zu k ist, und die Gleichungen (I) und (II) bleiben richtig, wenn man n alle relativen Primzahlen zu k, und q alle in k nicht aufgehenden Primzahlen durchlaufen lässt.

§. 133.

Es sei nun (wie in §. 131) k eine beliebige positive ganze Zahl, und zwar

$$k = 2^\lambda p^\pi p'^{\pi'} \ldots,$$

wo $p, p' \ldots$ von einander verschiedene ungerade Primzahlen bedeuten; wir geben ferner den Buchstaben

$$a,\ b,\ c,\ c' \ldots$$

ihre frühere Bedeutung (§. 131) und bezeichnen entsprechend mit

$$\theta,\ \eta,\ \omega,\ \omega' \ldots$$

irgend welche Wurzeln der Gleichungen

$$\theta^a = 1,\ \eta^b = 1,\ \omega^c = 1,\ \omega'^{c'} = 1 \ldots$$

Ist nun n irgend eine positive ganze Zahl und zugleich relative Primzahl zu k, und sind ihre Indices

$$\alpha \pmod a),\ \beta \pmod b),\ \gamma \pmod c),\ \gamma' \pmod{c'}) \ldots,$$

so genügt, wie man leicht sieht, der Ausdruck

$$\psi(n) = \frac{\theta^\alpha \eta^\beta \omega^\gamma \omega'^{\gamma'} \ldots}{n^s}$$

der Bedingung $\psi(n)\psi(n') = \psi(nn')$*); wenn ferner der Exponent $s > 1$ ist, was wir im Folgenden annehmen wollen, so ist die Summe der Moduln n^{-s} aller Glieder $\psi(n)$ endlich (§. 117), und folglich gelten die Gleichungen (I) und (II) des vorigen Paragraphen

$$\prod \frac{1}{1-\psi(q)} = \sum \psi(n) = L$$

$$\sum \psi(q) + \tfrac{1}{2} \sum \psi(q^2) + \tfrac{1}{3} \sum \psi(q^3) + \cdots = \log L$$

in welchen q alle in k nicht aufgehenden Primzahlen, n alle relativen Primzahlen zu k durchlaufen muss; beide Reihen haben, so lange $s > 1$ ist, bestimmte von der Anordnung ihrer Glieder un-

*) Der Zähler $\chi(n) = \theta^\alpha \eta^\beta \omega^\gamma \omega'^{\gamma'} \ldots$ besitzt die charakteristischen Eigenschaften $\chi(n)\chi(n') = \chi(nn')$ und, wenn $n' \equiv n'' \pmod k$ ist, $\chi(n') = \chi(n'')$. Umgekehrt, wenn eine Function $\chi(n)$ die erste Eigenschaft hat, und wenn sie ausserdem nur eine *endliche* Anzahl m (von Null verschiedener) Werthe $\omega_1, \omega_2 \ldots \omega_m$ besitzt, so sind diese letzteren nothwendig die sämmtlichen Wurzeln der Gleichung $\omega^m = 1$.

abhängige Summen. Wir können hinzufügen, dass beide Reihen auch *stetige* Functionen von s sind, so lange $s > 1$ ist; wir beweisen diese Behauptung für alle Werthe von s, welche grösser als ein beliebiger unechter Bruch σ sind, weil hieraus offenbar die Stetigkeit dieser Reihen für alle Werthe von $s > 1$ (excl. 1) folgt.

Jede der beiden Reihen L und $\log L$ ist von der Form

$$\frac{\alpha_1}{1^s} + \frac{\alpha_2}{2^s} + \frac{\alpha_3}{3^s} + \cdots,$$

wo die Moduln der Coefficienten $\alpha_1, \alpha_2, \alpha_3 \ldots$ sämmtlich eine endliche Grösse $A\,(=1)$ nicht übertreffen. Um die Stetigkeit einer Function von s innerhalb eines gewissen Intervalls $(s \geqq \sigma)$ zu beweisen, genügt es darzuthun, dass, wie klein auch eine positive gegebene Grösse δ sein mag, die Function jedesmal in einen ersten und zwar stetigen, und in einen zweiten Bestandtheil zerlegt werden kann, dessen Modulus innerhalb des ganzen Intervalls $(s \geqq \sigma)$ $< \delta$ ist; denn hieraus folgt, dass der Modulus einer plötzlichen Werthänderung der ganzen Function, die doch nur von dem zweiten Bestandtheil herrühren kann, kleiner als $2\,\delta$, und folglich, da die gegebene Grösse δ beliebig klein sein darf, nothwendig $= 0$ sein muss (vergl. §§. 101, 143). In unserm Falle ergiebt sich die Möglichkeit einer solchen Zerlegung auf folgende Weise; ist n eine beliebige ganze Zahl, so ist die Summe der ersten n Glieder

$$\frac{\alpha_1}{1^s} + \frac{\alpha_2}{2^s} + \cdots + \frac{\alpha_n}{n^s}$$

eine stetige Function; der Modulus der Summe aller folgenden Glieder ist kleiner als

$$A\left(\frac{1}{(n+1)^s} + \frac{1}{(n+2)^s} + \cdots\right)$$

und folglich für *alle* Werthe $s \geqq \sigma$ auch kleiner als

$$A\left(\frac{1}{(n+1)^\sigma} + \frac{1}{(n+2)^\sigma} + \cdots\right);$$

da nun σ ein unechter Bruch ist, und folglich (nach §. 117) die Reihe

$$\frac{1}{1^\sigma} + \frac{1}{2^\sigma} + \frac{1}{3^\sigma} + \cdots$$

convergirt, so kann für jede gegebene Grösse δ entsprechend n so gross gewählt werden, dass

$$A\left(\frac{1}{(n+1)^\sigma}+\frac{1}{(n+2)^\sigma}+\cdots\right)<\delta$$

wird; hiermit ist für jede gegebene Grösse δ die Möglichkeit einer Zerlegung unserer Reihe in zwei Bestandtheile von der obigen Art, und also auch die Stetigkeit der Reihen L und $\log L$ für jeden Werth $s>1$ nachgewiesen.

Der Beweis des Satzes über die arithmetische Progression gründet sich nun auf die Untersuchung des Verhaltens der Reihen L und $\log L$ bei unbegrenzter Annäherung des Exponenten s an den Werth 1. Wir bemerken zunächst, dass diese Reihen je nach der Wahl der in dem Ausdrucke $\psi(n)$ vorkommenden Einheits-Wurzeln θ, η, ω, ω' ... ein ganz verschiedenes Verhalten zeigen; da diese Wurzeln resp. a, b, c, c' ... verschiedene Werthe haben können, so sind in der Form L im Ganzen

$$a\,b\,c\,c'\ldots=\varphi(k)$$

verschiedene besondere Reihen enthalten; wir theilen diese Reihen L in drei Classen ein:

In die *erste* Classe nehmen wir nur eine einzige Reihe L_1 auf, und zwar diejenige, in welcher alle Einheits-Wurzeln θ, η, ω, ω'... den Werth $+1$ haben.

In die *zweite* Classe nehmen wir alle übrigen Reihen L_2 auf, in welchen alle Einheits-Wurzeln reelle Werthe, also die Werthe ± 1 haben.

In die *dritte* Classe nehmen wir alle übrigen Reihen L_3 auf, d. h. alle diejenigen, in welchen wenigstens eine der Einheits-Wurzeln imaginär ist. Die Anzahl dieser Reihen ist jedenfalls gerade, und sie sind paarweise mit einander conjugirt; denn entspricht eine solche Reihe L_3 den Wurzeln θ, η, ω, ω' ..., so entspricht immer eine zweite solche Reihe L'_3 den Wurzeln θ^{-1}, η^{-1}, ω^{-1}, ω'^{-1} ..., und diese beiden Systeme von Wurzeln sind nicht identisch.

Wir wollen nun das Verhalten aller dieser Reihen genau untersuchen, wenn der Exponent $s=1+\varrho$ sich dem Werthe 1 nähert, d. h. also, wenn die positive Grösse ϱ unendlich klein wird.

§. 134.

Betrachten wir zunächst das Verhalten der ersten Reihe

$$L_1 = \Sigma \frac{1}{n^s} = \Sigma \frac{1}{n^{1+\varrho}},$$

in welcher n alle relativen Primzahlen zu k durchlaufen muss, so leuchtet ein, dass dieselbe als ein Aggregat von $\varphi(k)$ Partialreihen von der Form

$$\frac{1}{v^{1+\varrho}} + \frac{1}{(v+k)^{1+\varrho}} + \frac{1}{(v+2k)^{1+\varrho}} + \cdots$$

angesehen werden kann, wo v relative Primzahl zu k und $\leqq k$ ist. Da nun (nach §. 117) das Product aus einer solchen Reihe und aus ϱ mit unendlich abnehmendem ϱ sich einem endlichen positiven, von Null verschiedenen Grenzwerth k^{-1} nähert, so können wir

$$L_1 = \frac{l}{\varrho}$$

setzen, wo l mit unendlich abnehmendem ϱ sich ebenfalls einem endlichen, positiven, von Null verschiedenen Grenzwerth nähert.

Ganz anders verhalten sich aber die Reihen L der zweiten und dritten Classe; wir haben gesehen, dass alle diese Reihen, so lange $s > 1$ ist, bestimmte von der Anordnung ihrer Glieder unabhängige Werthe besitzen; von jetzt an wollen wir aber ihre Glieder $\psi(n)$ so anordnen, dass die Zahlen n ihrer Grösse nach wachsend auf einander folgen; die so geordneten Reihen L der zweiten und dritten Classe *convergiren* dann für *alle positiven* Werthe von s und sind nebst ihren Derivirten auch *stetige* Functionen des positiven Exponenten s.

Um dies nachzuweisen, betrachten wir zunächst die ganze rationale Function

$$f(x) = \Sigma\, \theta^\alpha \eta^\beta \omega^\gamma \omega'^{\gamma'} \ldots x^\nu$$

der Variabeln x, wo das Summenzeichen sich auf diejenigen $\varphi(k)$ positiven ganzen Zahlen ν bezieht, die relative Primzahlen zu k und $< k$ sind, und wo $\alpha, \beta, \gamma, \gamma' \ldots$ die Indices der Zahl ν bedeuten. Setzt man $x = 1$, so erhält man

$$f(1) = \Sigma\, \theta^\alpha \eta^\beta \omega^\gamma \omega'^{\gamma'} \ldots,$$

wo die Indices $\alpha, \beta, \gamma, \gamma' \ldots$ unabhängig von einander vollständige Restsysteme resp. in Bezug auf die Moduln $a, b, c, c' \ldots$ durchlaufen müssen; es ist daher

$$f(1) = \Sigma\, \theta^{\alpha} . \Sigma\, \eta^{\beta} . \Sigma\, \omega\gamma . \Sigma\, \omega'\gamma' \ldots$$

Da nun nach unserer Voraussetzung die Reihe L eine Reihe der zweiten oder dritten Classe und folglich mindestens eine der Einheitswurzeln $\theta, \eta, \omega, \omega' \ldots$ *nicht* $= +1$ ist, so ist auch mindestens eine der Summen

$$\Sigma\, \theta^{\alpha},\ \Sigma\, \eta^{\beta},\ \Sigma\, \omega\gamma,\ \Sigma\, \omega'\gamma' \ldots$$

gleich Null, und hieraus folgt

$$f(1) = 0.$$

Mit Hülfe dieses Resultates kann man nun die oben behaupteten Eigenschaften der Reihen L auf verschiedene Arten nachweisen. Die eine besteht darin, dass man die Reihe L in ein bestimmtes Integral verwandelt. Nach der von *Legendre* eingeführten Bezeichnung ist

$$\Gamma(s) = \int_0^1 \left(\log \frac{1}{x}\right)^{s-1} dx$$

eine für alle positiven Werthe von s endliche und stetige Function von s; bedeutet ferner n irgend einen positiven Werth, und ersetzt man x durch x^n, so ergiebt sich

$$\frac{\Gamma(s)}{n^s} = \int_0^1 x^{n-1} \left(\log \frac{1}{x}\right)^{s-1} dx;$$

und hieraus folgt leicht (ähnlich wie in den §§. 103, 105), dass die Summe der *ersten* $m\varphi(k)$ Glieder der Reihe L gleich

$$\frac{1}{\Gamma(s)} \int_0^1 \frac{1}{x} \frac{f(x)}{1-x^k} \left(\log \frac{1}{x}\right)^{s-1} (1 - x^{mk})\, dx$$

ist. Da nun $f(x)$ eine durch x theilbare ganze Function von x ist, welche für $x = 1$ verschwindet, so bleibt innerhalb des ganzen Integrationsgebietes der Modulus der Function

$$\frac{1}{x} \frac{f(x)}{1-x^k}$$

unterhalb einer angebbaren endlichen Grösse, und hieraus folgt leicht, wenn man m unendlich wachsen lässt, dass

$$L = \frac{1}{\Gamma(s)} \int_0^1 \frac{1}{x} \frac{f(x)}{1-x^k} \left(\log \frac{1}{x}\right)^{s-1} dx$$

ist. Es zeigt sich also in der That, dass die unendliche Reihe L der zweiten oder dritten Classe, wenn ihre Glieder in der angegebenen Weise geordnet sind, für jeden positiven Werth von s *convergirt*; beachtet man ferner, dass $\Gamma(s)$ für alle positiven Werthe von s ebenfalls positiv und von Null verschieden, sowie, dass die Derivirte von $\Gamma(s)$ eine stetige Function von s ist, so folgt aus dem vorstehenden geschlossenen Ausdruck für die Reihe L, dass dieselbe nebst ihrer Derivirten eine *stetige* Function von s ist, so lange s positiv bleibt.

Zu demselben Resultate gelangt man aber auch auf anderm Wege, nämlich mit Hülfe des weiter unten in §. 143 bewiesenen allgemeinen Satzes. Denn da zufolge der Gleichung $f(1) = 0$ die Summe der Coefficienten

$$\theta^\alpha \eta^\beta \omega^\gamma \omega'^{\gamma'} \ldots$$

von je $\varphi(k)$ auf einander folgenden Gliedern der Reihe L den Werth Null hat, so bildet die Reihe L eine solche unendliche Reihe, wie sie in §. 143 betrachtet wird; man braucht dort nur unter $k_1, k_2, k_3 \ldots$ die Werthe der successiven Zahlen n zu verstehen, so ergeben sich unmittelbar unsere obigen Behauptungen über die Convergenz und Stetigkeit der Reihe L und ihrer Derivirten.

Aus diesem Resultat ergiebt sich nun, dass jede Reihe L der zweiten oder dritten Classe, wenn der Exponent $s = 1 + \varrho$ abnehmend dem Werth 1 unendlich nahe kommt, sich einem völlig bestimmten *endlichen* Grenzwerth, nämlich dem Werth

$$\int_0^1 \frac{1}{x} \frac{f(x)}{1-x^k} dx$$

nähert, welchen die Reihe L bei der oben angegebenen Anordnung ihrer Glieder für $s = 1$ annimmt.

§. 135.

Es hat nun zwar gar keine Schwierigkeit, den Werth des vorstehenden Integrals mit Hülfe von Logarithmen und Kreisfunctionen darzustellen*); dass aber dieser endliche Grenzwerth einer Reihe L der zweiten oder dritten Classe *von Null verschieden* ist — und gerade hierin besteht der Hauptpunct der ganzen nachfolgenden Untersuchung — würde sich aus diesem Ausdrucke schwer oder gar nicht erkennen lassen. Es ist nun von dem höchsten Interesse, dass dieser Nachweis für die Reihen L_2 der zweiten Classe sich mit Hülfe der Untersuchungen des fünften Abschnitts über die Classenanzahl der quadratischen Formen führen lässt; ja wir können hinzufügen, dass historisch jene Untersuchungen ihren Ausgangspunct an dieser Stelle genommen haben.

Wir betrachten eine bestimmte Reihe L_2 der zweiten Classe, welche den Wurzeln

$$\theta = \pm 1, \quad \eta = \pm 1, \quad \omega = \pm 1, \quad \omega' = \pm 1 \ldots$$

entspricht; es sei P das Product aller der in k aufgehenden ungeraden Primzahlen p, denen eine negative Wurzel $\omega = -1$ entspricht, und S das Product der übrigen in k aufgehenden ungeraden Primzahlen (falls in der einen oder andern dieser beiden Gruppen gar keine Primzahl enthalten sein sollte, ist P oder $S = 1$ zu setzen); da nun eine Zahl n quadratischer Rest oder Nichtrest einer Primzahl ist, je nachdem ihr Index γ gerade oder ungerade ist (§. 129), so leuchtet ein, dass

$$\omega^\gamma \omega'^{\gamma'} \ldots = \left(\frac{n}{P}\right)$$

ist; wenn ferner $\theta = -1$, also $a = 2$, und $k \equiv 0 \pmod 4$ ist, so sind alle Zahlen n ungerade, und es ist (nach §. 130)

$$\theta^\alpha = (-1)^\alpha = (-1)^{\frac{1}{2}(n-1)};$$

*) Bei der wirklichen Ausführung der Rechnung durch Zerlegung in Partialbrüche (ähnlich wie in den §§. 103, 105) würde man auf die in der Theorie der Kreistheilung vorkommenden Summen $f(r)$ stossen, wo r irgend eine Wurzel der Gleichung $r^k = 1$ bedeutet.

ebenso, wenn $\eta = -1$, also $b > 1$, und $k \equiv 0 \pmod 8$ ist, so sind alle Zahlen n ungerade, und es ist (nach §. 130)

$$\eta^\beta = (-1)^\beta = (-1)^{\frac{1}{8}(n^2-1)}.$$

Diese Bemerkungen veranlassen uns (vergl. §§. 101, 123), je nach den vier verschiedenen Zeichencombinationen θ, η vier verschiedene Determinanten D zu betrachten; wir setzen nämlich, mit gehöriger Rücksicht auf das Zeichen ± 1:

$$\begin{aligned}
D &= \pm\ PS^2 \equiv 1 \pmod 4, \quad \text{wenn} \quad \theta = +1, \quad \eta = +1 \\
D &= \pm\ PS^2 \equiv 3 \pmod 4, \quad \text{wenn} \quad \theta = -1, \quad \eta = +1 \\
D &= \pm 2PS^2 \equiv 2 \pmod 8, \quad \text{wenn} \quad \theta = +1, \quad \eta = -1 \\
D &= \pm 2PS^2 \equiv 6 \pmod 8, \quad \text{wenn} \quad \theta = -1, \quad \eta = -1.
\end{aligned}$$

Nun sind alle ungeraden Zahlen n auch relative Primzahlen zu $2D$, und umgekehrt, alle relativen Primzahlen zu $2D$ sind auch ungerade Zahlen n, und gleichzeitig ist

$$\theta^\alpha \eta^\beta \omega^\gamma \omega'^{\gamma'} \ldots = \theta^{\frac{1}{8}(n-1)} \eta^{\frac{1}{8}(n^2-1)} \left(\frac{n}{P}\right) = \left(\frac{D}{n}\right);$$

ist daher k gerade, so stimmen die sämmtlichen Zahlen n mit den sämmtlichen relativen Primzahlen zu $2D$ überein, und es ist

$$L_2 = \Sigma\, \psi(n) = \Sigma \left(\frac{D}{n}\right) \frac{1}{n^s};$$

ist aber k ungerade, so sind unter den Zahlen n auch gerade Zahlen; da in diesem Falle aber nothwendig $\theta = +1$, $\eta = +1$, also $D \equiv 1 \pmod 4$ ist, so ist (vergl. §. 102)

$$L_2 = \Sigma \left(\frac{n}{P}\right) \frac{1}{n^s} = \frac{1}{1 - \left(\frac{2}{P}\right) \frac{1}{2^s}} \Sigma \left(\frac{D}{n}\right) \frac{1}{n^s},$$

wo in der letzten Summe rechter Hand der Buchstabe n nur noch alle ungeraden relativen Primzahlen zu k, d. h. alle relativen Primzahlen zu $2D$ zu durchlaufen hat.

Um daher zu beweisen, dass die Reihe L_2 sich einem von Null verschiedenen Grenzwerth nähert, braucht man dasselbe nur von der Reihe

$$\Sigma \left(\frac{D}{n}\right) \frac{1}{n^s}$$

nachzuweisen. Nun leuchtet ein, dass die Zahl D nie eine *Quadratzahl* sein kann; denn da eine Quadratzahl niemals $\equiv 3 \pmod 4$,

oder $\equiv 2 \pmod 8$ oder $\equiv 6 \pmod 8$ ist, so bleibt nur die einzige Möglichkeit $D \equiv 1 \pmod 4$; da aber in diesem Falle $\theta = +1$, $\eta = +1$ ist, so muss, da L_2 eine Reihe der zweiten Classe ist, wenigstens eine der Wurzeln $\omega, \omega' \ldots = -1$ sein, und folglich P mindestens durch eine ungerade Primzahl p theilbar, also nicht $= 1$ sein; mithin ist D in keinem Falle eine Quadratzahl. Wir haben nun (in §§. 96 und 98) gesehen, dass die Anzahl h der Classen nicht äquivalenter ursprünglicher Formen von der (nicht quadratischen) Determinante D ein Product aus mehreren Factoren ist, von denen der eine der Grenzwerth der obigen Reihe

$$\Sigma \left(\frac{D}{n}\right) \frac{1}{n^s}$$

ist; da nun immer mindestens eine Form $(1, 0, -D)$ existirt, also h niemals $= 0$ ist, und da ferner die übrigen in dem Ausdruck von h vorkommenden Factoren nicht unendlich gross sind, so ist auch dieser Grenzwerth von Null verschieden. Und hieraus folgt, dass auch der Grenzwerth einer jeden Reihe L_2 der zweiten Classe ein von Null verschiedener und folglich positiver Werth ist, was zu beweisen war.

In dem einfachsten Falle, wo k eine Potenz einer ungeraden Primzahl p oder das Doppelte einer solchen Potenz ist, existirt nur eine Reihe

$$L_2 = \Sigma \left(\frac{n}{p}\right) \frac{1}{n^s}$$

der zweiten Classe; in diesem Falle bedarf es nicht der Zuziehung der Theorie der quadratischen Formen, um nachzuweisen, dass der Grenzwerth

$$\Sigma \left(\frac{n}{p}\right) \frac{1}{n}$$

dieser Reihe von Null verschieden ist; für diese Summe haben wir nämlich in §. 103 einen Ausdruck gefunden, welcher neben solchen Factoren, die offenbar von Null verschieden sind, noch den Factor

$$\Sigma \left(\frac{m}{p}\right) m \quad \text{oder} \quad \Sigma \left(\frac{m}{p}\right) \log \sin \frac{m\pi}{p}$$

enthält, je nachdem $p \equiv 3$ oder $\equiv 1 \pmod 4$ ist, und wo m alle Zahlen $1, 2, 3 \ldots (p-1)$ durchlaufen muss. Im ersten Fall ist aber Σm und folglich auch

$$\Sigma \left(\frac{m}{p}\right) m$$

ungerade, also von Null verschieden; im zweiten Fall ist (§. 107)

$$-\Sigma \left(\frac{m}{p}\right) \log \sin \frac{m\pi}{p} = \log \frac{y + z\sqrt{p}}{y - z\sqrt{p}},$$

wo die ganzen Zahlen y, z der Gleichung $y^2 - pz^2 = 4p$ genügen; es kann folglich z, und also auch der vorstehende Ausdruck nicht $= 0$ sein.

§. 136.

Um nun dasselbe auch für jede Reihe L_3 der dritten Classe zu beweisen, addiren wir alle $\varphi(k)$ Gleichungen von der Form

$$\Sigma \psi(q) + \tfrac{1}{2} \Sigma \psi(q^2) + \tfrac{1}{3} \Sigma \psi(q^3) + \cdots = \log L,$$

welche den verschiedenen Wurzel-Systemen θ, η, ω, $\omega' \ldots$ entsprechen. Bedeutet q irgend eine in k nicht aufgehende Primzahl, und μ irgend eine positive ganze Zahl, so liefert die linke Seite einer jeden solchen Gleichung ein Glied

$$\frac{1}{\mu} \psi(q^\mu),$$

in welchem

$$\frac{1}{\mu} \frac{1}{q^{\mu s}}$$

mit dem Coefficienten

$$\theta^{\alpha\mu} \eta^{\beta\mu} \omega^{\gamma\mu} \omega'^{\gamma'\mu} \ldots$$

behaftet ist, wo α, β, γ, $\gamma' \ldots$ die Indices von q bedeuten. Die Summe aller dieser den verschiedenen Wurzelsystemen θ, η, ω, $\omega' \ldots$ entsprechenden Coefficienten wird daher gleich dem Product

$$\Sigma \theta^{\alpha\mu} \Sigma \eta^{\beta\mu} \Sigma \omega^{\gamma\mu} \Sigma \omega'^{\gamma'\mu} \ldots,$$

wo die Summenzeichen sich der Reihe nach auf die a, b, c, $c' \ldots$ verschiedenen Werthe von θ, η, ω, $\omega' \ldots$ beziehen. Bekanntlich ist nun die Summe aller gleich hohen Potenzen der Wurzeln von einer Gleichung der Form $x^m = 1$ nur dann von Null verschieden,

und zwar $= m$, wenn der Exponent dieser Potenzen durch m theilbar ist; mithin ist das vorstehende Product nur dann von Null verschieden, und zwar $= abcc' \ldots = \varphi(k)$, wenn die Exponenten $\alpha\mu$, $\beta\mu$, $\gamma\mu$, $\gamma'\mu \ldots$ resp. durch a, b, c, $c' \ldots$ theilbar sind; da nun $\alpha\mu$, $\beta\mu$, $\gamma\mu$, $\gamma'\mu \ldots$ die Indices von q^μ sind, so wird dies nur dann und immer dann eintreten, wenn

$$q^\mu \equiv 1 \pmod{2^\lambda}, \quad q^\mu \equiv 1 \pmod{p^\pi}, \quad q^\mu \equiv 1 \pmod{p'^{\pi'}} \ldots,$$

d. h. also, wenn

$$q^\mu \equiv 1 \pmod{k}$$

ist. Mithin wird die Summe aller jener Gleichungen folgende Form annehmen

$$\varphi(k)\left\{\Sigma\frac{1}{q^s} + \tfrac{1}{2}\Sigma\frac{1}{q^{2s}} + \cdots + \frac{1}{\mu}\Sigma\frac{1}{q^{\mu s}} + \cdots\right\}$$
$$= \log L_1 + \Sigma \log L_2 + \Sigma \log (L_3 L'_3),$$

wo auf der linken Seite das erste, zweite Summenzeichen u. s. f. sich auf alle die in k nicht aufgehenden Primzahlen q bezieht, welche resp. den Bedingungen $q \equiv 1$, $q^2 \equiv 1 \pmod{k}$ u. s. f. Genüge leisten; auf der rechten Seite bezieht sich das erste Summenzeichen auf alle Reihen L_2 der zweiten Classe, das zweite auf alle verschiedenen Paare $L_3 L'_3$ conjugirter Reihen dritter Classe. Mit Hülfe dieser Gleichung sind wir im Stande zu beweisen, dass der endliche Grenzwerth, welchem sich irgend eine Reihe L_3 der dritten Classe nähert, von Null verschieden ist.

Dieser Beweis stützt sich auf das schon früher (§. 134) erhaltene Resultat, dass jede solche Reihe L_3 für alle positiven Werthe von s eine stetige Function von s ist, und dass dasselbe auch von ihrer Derivirten gilt. Wir können daher

$$L_3 = f(s) + iF(s)$$
$$L'_3 = f(s) - iF(s)$$

setzen, wo $f(s)$, $F(s)$ und die Derivirten $f'(s)$, $F'(s)$ stetige Functionen von s sind, so lange s positiv bleibt; da also der Grenzwerth von $L_3 = f(1) + iF(1)$ ist, so muss, falls derselbe $= 0$ ist, nothwendig $f(1) = 0$ und $F(1) = 0$ sein; hieraus folgt nach einem bekannten Satze der Differentialrechnung, dass für jeden Werth $s = 1 + \varrho$, welcher > 1 ist,

$$L_3 = \varrho\,\{f'(1+\delta\varrho) + iF'(1+\varepsilon\varrho)\}$$
$$L'_3 = \varrho\,\{f'(1+\delta\varrho) - iF'(1+\varepsilon\varrho)\}$$

sein wird, wo δ und ε zwischen den Grenzen 0 und 1 liegen; mithin wird

$$L_3 L'_3 = \varrho^2\,\{f'(1+\delta\varrho)^2 + F'(1+\varepsilon\varrho)^2\} = \varrho^2 R,$$

wo R (in Folge der Endlichkeit und Stetigkeit der Derivirten $f'(s)$, $F'(s)$) mit unendlich abnehmendem positiven ϱ sich einem endlichen (nicht negativen) Grenzwerth

$$f'(1)^2 + F'(1)^2$$

nähert. Hieraus folgt nun

$$\log(L_3 L'_3) = -2\log\frac{1}{\varrho} + \log R,$$

wo $\log R$ mit unendlich abnehmendem ϱ sich entweder einem endlichen Grenzwerth nähert oder negativ über alle Grenzen wächst, falls R unendlich klein wird.

Sind im Ganzen m solche Paare von Reihen dritter Classe vorhanden, welche gleichzeitig mit ϱ unendlich klein werden, so ist folglich

$$\Sigma \log(L_3 L'_3) = -2m\log\frac{1}{\varrho} + t,$$

wo t jedenfalls nicht positiv über alle Grenzen wachsen kann, sondern entweder endlich bleibt, oder negativ über alle Grenzen wächst; denn da jedes Product $L_3 L'_3$ sich einem endlichen nicht negativen Werth nähert, so kann auch kein Glied $\log(L_3 L'_3)$ positiv über alle Grenzen wachsen.

Da ferner schon gezeigt ist, dass der Grenzwerth einer jeden Reihe L_2 der zweiten Classe von Null verschieden ist, so nähert sich die Summe

$$\Sigma \log L_2$$

der (jedenfalls reellen) Reihen $\log L_2$ einem endlichen Grenzwerth.

Ausserdem ist schon bewiesen, dass das Product ϱL_1 sich einem endlichen von Null verschiedenen Werth nähert; mithin ist

$$\log L_1 = \log\frac{1}{\varrho} + t',$$

wo t' endlich bleibt; folglich ist die ganze rechte Seite der obigen Gleichung von der Form

$$-(2m-1)\log\frac{1}{\varrho}+T,$$

wo T mit unendlich abnehmendem ϱ jedenfalls nicht positiv über alle Grenzen wachsen kann. Existirte also mindestens eine Reihe L_3 dritter Classe, welche mit ϱ unendlich klein würde, d. h. wäre m mindestens $=1$, so würde die ganze rechte Seite unserer Gleichung mit unendlich abnehmendem positiven ϱ *negativ* unendlich wachsen. Dies ist aber unmöglich, da die linke Seite für alle Werthe von ϱ positiv bleibt. Mithin ist $m=0$, d. h. jede Reihe der dritten Classe nähert sich einem von Null verschiedenen Grenzwerth, was zu beweisen war.

Hieraus folgt endlich noch, dass auch jede der Reihen $\log L_3$ einen endlichen Grenzwerth haben muss, wenn man berücksichtigt, dass nach dem früher Bewiesenen (§. 133) jede solche Reihe sich stetig mit s ändert, so lange $s>1$ ist.

§. 137.

Das Resultat der vorhergehenden Untersuchungen besteht darin, dass bei dem unendlichen Abnehmen der positiven Grösse $\varrho=s-1$ die Reihe $\log L_1$ positiv über alle Grenzen wächst, während alle übrigen Reihen $\log L$ sich endlichen Grenzwerthen nähern. Mit Hülfe desselben sind wir im Stande, den Satz über die arithmetische Progression vollständig zu beweisen.

Es sei nämlich m irgend eine relative Primzahl zu k, so multipliciren wir jede der $\varphi(k)$ Reihen von der Form

$$\Sigma\,\psi(q)+\tfrac{1}{2}\Sigma\,\psi(q^2)+\tfrac{1}{3}\Sigma\,\psi(q^3)+\cdots=\log L,$$

welche einem bestimmten System von Einheits-Wurzeln θ, η, ω, ω' ... entspricht, mit dem correspondirenden Werth

$$\theta^{-\alpha_1}\eta^{-\beta_1}\omega^{-\gamma_1}\omega'^{-\gamma_1'}\ldots=\chi,$$

wo α_1, β_1, γ_1, γ_1' ... die Indices der Zahl m bedeuten, und addiren alle Producte; dann wird, wenn wieder α, β, γ, γ' ... die Indices einer bestimmten Primzahl q sind, das Glied

$$\frac{1}{\mu}\,\frac{1}{q^{\mu s}}$$

den Coefficienten

$$\Sigma\, \theta^{\alpha\mu-\alpha_1}\, \eta^{\beta\mu-\beta_1}\, \omega^{\gamma\mu-\gamma_1}\, \omega'^{\gamma'\mu-\gamma_1'} \ldots$$

erhalten, wo sich das Summenzeichen auf alle $\varphi(k)$ Wurzel-Systeme bezieht; dieser Coefficient ist daher auch gleich dem Product aus den einzelnen Summen

$$\Sigma\, \theta^{\alpha\mu-\alpha_1},\ \Sigma\, \eta^{\beta\mu-\beta_1},\ \Sigma\, \omega^{\gamma\mu-\gamma_1},\ \Sigma\, \omega'^{\gamma'\mu-\gamma_1'} \ldots,$$

in welchen die Buchstaben $\theta, \eta, \omega, \omega' \ldots$ resp. ihre $a, b, c, c' \ldots$ verschiedenen Werthe durchlaufen müssen; dieser Coefficient wird folglich nur dann von Null verschieden, und zwar $= abcc' \ldots = \varphi(k)$ sein, wenn die Exponenten $\alpha\mu - \alpha_1$, $\beta\mu - \beta_1$, $\gamma\mu - \gamma_1$, $\gamma'\mu - \gamma_1' \ldots$ resp. durch $a, b, c, c' \ldots$ theilbar sind, d. h. wenn

$$q^\mu \equiv m \pmod{k}$$

ist. Die Summation aller Producte $\chi \log L$ giebt daher das Resultat

$$\varphi(k)\left\{\Sigma\frac{1}{q^s}+\tfrac{1}{2}\Sigma\frac{1}{q^{2s}}+\tfrac{1}{3}\Sigma\frac{1}{q^{3s}}+\ldots\right\} = \Sigma\,\chi\log L,$$

wo auf der linken Seite das erste, zweite, dritte Summenzeichen u. s. f. sich auf alle Primzahlen q bezieht, welche resp. den Bedingungen $q \equiv m$, $q^2 \equiv m$, $q^3 \equiv m \pmod{k}$ u. s. f. genügen, während das Summenzeichen auf der rechten Seite sich auf die sämmtlichen $\varphi(k)$ verschiedenen Wurzel-Systeme $\theta, \eta, \omega, \omega' \ldots$ bezieht. Bezeichnet man nun mit z alle positiven ganzen Zahlen mit Ausnahme von 1, so ist offenbar

$$\tfrac{1}{2}\Sigma\frac{1}{q^{2s}}+\tfrac{1}{3}\Sigma\frac{1}{q^{3s}}+\tfrac{1}{4}\Sigma\frac{1}{q^{4s}}+\ldots = Q$$

kleiner als

$$\tfrac{1}{2}\Sigma\frac{1}{z^2}+\tfrac{1}{2}\Sigma\frac{1}{z^3}+\tfrac{1}{2}\Sigma\frac{1}{z^4}+\ldots,$$

wo in jeder Summe z alle seine Werthe durchläuft; da nun, sobald $z \geqq 2$, immer

$$\frac{1}{z^3} \leqq \frac{1}{2}\frac{1}{z^2},\quad \frac{1}{z^4} \leqq \frac{1}{4}\frac{1}{z^2},\quad \frac{1}{z^5} \leqq \frac{1}{8}\frac{1}{z^2}\ldots$$

ist, so ergiebt sich

$$Q < \Sigma\frac{1}{z^2};$$

während daher s abnehmend sich dem Werthe 1 nähert, bleibt Q fortwährend unterhalb einer endlichen Grösse. Da ferner alle Glieder $\chi \log L$ sich endlichen Grenzwerthen nähern, mit Ausnahme des einzigen Gliedes $\log L_1$, welches über alle Grenzen wächst, so muss auch die Summe

$$\Sigma \frac{1}{q^s}$$

über alle Grenzen wachsen; dies wäre aber nicht möglich, wenn diese Summe aus einer endlichen Anzahl von Gliedern bestände, und folglich muss es unendlich viele Primzahlen q geben, welche $\equiv m \pmod{k}$ sind; d. h. also:

*Jede unbegrenzte arithmetische Progression $kx + m$, deren Anfangsglied m und Differenz k relative Primzahlen sind, enthält unendlich viele positive Primzahlen q *).*

*) Ueber die Ausdehnung dieses Satzes auf Linearformen mit complexen Coefficienten, sowie auf quadratische Formen siehe *Dirichlet: Untersuchungen über die Theorie der complexen Zahlen*, Abhandlungen der Berliner Akademie aus dem Jahre 1841; Monatsbericht der Berliner Akademie (März 1840) oder Crelle's Journal XXI; Comptes rendus der Pariser Akademie 1849, T. X, p. 285.

VII. Ueber einige Sätze aus der Theorie der Kreistheilung.

§. 138.

Sind $p, p', p'' \ldots$ positive und von einander verschiedene Primzahlen, so stimmen (nach §. 9) die Glieder des entwickelten Productes

$$(p+1)\,(p'+1)\,(p''+1)\ldots$$

mit den sämmtlichen Divisoren des Productes

$$P = pp'p''\ldots$$

überein; dieselben Divisoren entstehen offenbar auch durch die Entwicklung des Productes

$$(p-1)\,(p'-1)\,(p''-1)\ldots,$$

aber die eine Hälfte derselben wird mit positivem, die andere mit negativem Zeichen behaftet sein; wir wollen die erstern mit δ_1, die letztern mit δ_2 bezeichnen, so dass

$$(p-1)\,(p'-1)\,(p''-1)\ldots = \Sigma\,\delta_1 - \Sigma\,\delta_2$$

wird, und wir bemerken, dass die Zahl P selbst zu der Classe der erstern gehört. Ist nun δ irgend ein Divisor von P, aber $< P$, so lässt sich leicht zeigen, dass die Anzahl der durch δ theilbaren Zahlen δ_1 genau gleich der Anzahl der durch δ theilbaren Zahlen δ_2 ist. Denn wenn man mit $q, q', q'' \ldots$ alle diejenigen Primfactoren von P bezeichnet, welche nicht in δ aufgehen, so stimmen die durch δ theilbaren Zahlen δ_1 und $-\delta_2$ resp. mit den positiven und negativen Gliedern des entwickelten Productes

$$\delta(q-1)(q'-1)(q''-1)\ldots$$

überein, und da $\delta < P$ ist, also mindestens eine solche Primzahl q vorhanden ist, so ist die Anzahl der positiven Glieder dieses Productes genau gleich der Anzahl der negativen.

Dieser Satz lässt sich leicht verallgemeinern. Bedeutet m irgend eine positive ganze Zahl > 1, und sind $p, p', p'' \ldots$ die sämmtlichen von einander verschiedenen in m aufgehenden positiven Primzahlen, so kann man

$$m\left(1-\frac{1}{p}\right)\left(1-\frac{1}{p'}\right)\left(1-\frac{1}{p''}\right)\cdots = \Sigma\,\mu_1 - \Sigma\,\mu_2$$

setzen, wo mit μ_1 und $-\mu_2$ resp. alle positiven und negativen Glieder des entwickelten Productes linker Hand bezeichnet sind. Behält man die vorhergehenden Bezeichnungen bei, so stimmen offenbar die Zahlen μ_1 und μ_2 resp. mit den Zahlen $m'\delta_1$ und $m'\delta_2$ überein, wenn zur Abkürzung $m = m'P$ gesetzt wird. Bedeutet nun μ irgend einen Divisor von m, mit Ausnahme von m selbst, so folgt hieraus wieder, dass unter den Zahlen μ_1 ebenso viele durch μ theilbar sein werden, wie unter den Zahlen μ_2. Denn, wenn μ' der grösste gemeinschaftliche Divisor von μ und m' ist, so kann man $\mu = \mu'\delta$ setzen, wo δ nothwendig ein Divisor von P, und zwar $< P$ sein muss; und da eine Zahl $\mu_1 = m'\delta_1$ oder $\mu_2 = m'\delta_2$ stets und nur dann durch $\mu = \mu'\delta$ theilbar ist, sobald resp. δ_1 oder δ_2 durch δ theilbar ist, so ergiebt sich in der That, dass die Anzahl der durch μ theilbaren Zahlen μ_1 genau gleich der Anzahl der durch μ theilbaren Zahlen μ_2 ist.

Von dieser Eigenschaft der Zahlen μ_1 und μ_2 kann man vielfache Anwendungen machen. Hängen z. B. zwei Functionen $f(m)$ und $F(m)$ einer beliebigen ganzen Zahl m durch eine der beiden Relationen

$$\Sigma f(\mu) = F(m)$$

oder

$$\Pi f(\mu) = F(m)$$

zusammen, wo das Summen- oder Productzeichen sich jedesmal auf alle Divisoren μ (incl. m) der Zahl m bezieht, so folgt daraus resp. die Umkehrung

$$f(m) = \Sigma F(\mu_1) - \Sigma F(\mu_2)$$

oder

$$f(m) = \frac{\Pi F(\mu_1)}{\Pi F(\mu_2)},$$

wo die Summen- oder Productzeichen sich auf alle Werthe von μ_1 oder auf alle Werthe von μ_2 beziehen; denn ersetzt man rechts jeden Werth $F(\mu_1)$ und $F(\mu_2)$ durch die Summe oder das Product der Werthe $f(\mu)$, die den sämmtlichen Divisoren μ von μ_1 oder μ_2 entsprechen, so werden zufolge der obigen Eigenschaft der Zahlen μ_1, μ_2 alle Werthe $f(\mu)$ sich aufheben, in welchen $\mu < m$ ist, und es wird allein der Werth $f(m)$ zurückbleiben.

Als Beispiel wählen wir die Aufgabe, die Anzahl $\varphi(m)$ der ganzen Zahlen zu bestimmen, welche relative Primzahlen zu m und nicht grösser als m sind; aus dieser Definition der Function $\varphi(m)$ ist in §. 13 ohne alle Rechnung der Satz abgeleitet, dass

$$\Sigma\, \varphi(\mu) = m$$

ist, wo das Summenzeichen sich auf alle Divisoren μ von m bezieht; setzen wir daher $F(m) = m$, so ergiebt sich umgekehrt

$$\varphi(m) = \Sigma\, \mu_1 - \Sigma\, \mu_2,$$

also

$$\varphi(m) = m\left(1-\frac{1}{p}\right)\left(1-\frac{1}{p'}\right)\left(1-\frac{1}{p''}\right)\cdots;$$

diese Function ist daher durch den Satz des §. 13 schon vollständig charakterisirt.

Ein anderes Beispiel ist folgendes. Ist der Werth der Function $f(m) = p$, sobald die Zahl m eine Potenz einer Primzahl p ist, dagegen $= 1$, so oft $m = 1$ oder durch mehrere verschiedene Primzahlen theilbar ist, so leuchtet ein, dass

$$\Pi f(\mu) = m$$

ist, wo das Productzeichen sich auf alle Divisoren μ von m bezieht; hieraus folgt nach dem obigen Satze, dass umgekehrt der Quotient

$$\frac{\Pi \mu_1}{\Pi \mu_2} = f(m),$$

also nur dann von 1 verschieden ist, wenn m eine Potenz einer Primzahl ist; und zwar ist dieser Quotient dann gleich dieser Primzahl.

Aus der Definition der Divisoren μ_1 und μ_2 folgt endlich auch, dass stets

$$\psi(m')\,(\psi(p)-1)\,(\psi(p')-1)\,(\psi(p'')-1)\ldots = \Sigma\,\psi(\mu_1) - \Sigma\,\psi(\mu_2)$$

ist, wenn die Function ψ die Eigenschaft $\psi(z)\,\psi(z') = \psi(zz')$ besitzt.

§. 139.

Die sämmtlichen Wurzeln ϱ der Gleichung

$$x^m = 1 \tag{1}$$

sind bekanntlich in der Form enthalten

$$\varrho = \cos\frac{2n\pi}{m} + i\sin\frac{2n\pi}{m},$$

wo n irgend ein vollständiges Restsystem (mod. m) durchlaufen muss.

Ist n relative Primzahl zu m, so sind die Potenzen

$$1, \varrho, \varrho^2 \ldots \varrho^{m-1}$$

sämmtlich ungleich, und sie bilden die sämmtlichen Wurzeln der obigen Gleichung (1); ϱ heisst in diesem Fall eine *primitive* Wurzel dieser Gleichung, und die Anzahl dieser primitiven Wurzeln ist offenbar $= \varphi(m)$. Ist allgemeiner ν der grösste gemeinschaftliche Divisor von n und $m = \mu\nu$, so ist ϱ eine primitive Wurzel der Gleichung

$$x^\mu = 1, \tag{2}$$

und da umgekehrt jede Wurzel der letztern Gleichung (2) auch eine Wurzel der Gleichung (1) ist, so leuchtet ein, dass die sämmtlichen Wurzeln der Gleichung (1) identisch sind mit allen primitiven Wurzeln aller der Gleichungen (2), die den sämmtlichen Divisoren μ der Zahl m entsprechen. Bezeichnet man daher mit ϱ' alle $\varphi(\mu)$ primitiven Wurzeln der Gleichung (2), und setzt

$$f(\mu) = \Pi\,(x - \varrho'),$$

wo das Productzeichen sich auf alle Wurzeln ϱ' bezieht, so ist

$$\Pi f(\mu) = x^m - 1,$$

wo das Productzeichen sich auf alle Divisoren μ der Zahl m bezieht; durch Umkehrung dieser für jede Zahl m geltenden Relation erhält man nach dem vorhergehenden Paragraphen

$$f(m) = \frac{\Pi\,(x^{\mu_1} - 1)}{\Pi\,(x^{\mu_2} - 1)},$$

woraus folgt, dass die Coefficienten der Function $f(m)$ sämmtlich ganze rationale Zahlen sind.

Von jetzt an betrachten wir nur noch den Fall, in welchem $m = P = pp'p'' \ldots$ eine ungerade und durch kein Quadrat theilbare ganze Zahl > 1 ist. Dann wird

$$\varphi(P) = (p-1)(p'-1)(p''-1)\ldots = \Sigma\mu_1 - \Sigma\mu_2$$

eine gerade Zahl, die wir mit 2τ bezeichnen wollen, und die sämmtlichen 2τ relativen Primzahlen zu P, welche $< P$ sind, zerfallen in τ Zahlen a und in τ Zahlen b von der Beschaffenheit, dass

$$\left(\frac{a}{P}\right) = +1, \quad \left(\frac{b}{P}\right) = -1$$

ist (§. 52. I. oder Supplemente §. 116). Setzen wir daher

$$\theta = \cos\frac{2\pi}{P} + i\sin\frac{2\pi}{P} = e^{\frac{2\pi i}{P}}$$

und

$$A(x) = \Pi(x-\theta^a), \quad B(x) = \Pi(x-\theta^b),$$

so wird

$$A(x)\,B(x) = \frac{\Pi(x^{\mu_1}-1)}{\Pi(x^{\mu_2}-1)},$$

und wir wollen im Folgenden die allgemeine Form der Coefficienten der Functionen $A(x)$, $B(x)$ bestimmen.

Zu diesem Zwecke erinnern wir zunächst an die Newton'schen Formeln, welche dazu dienen, aus den Coefficienten einer Gleichung die Summen gleich hoher Potenzen ihrer Wurzeln, und umgekehrt aus diesen jene abzuleiten. Es seien

$$w_1, w_2 \ldots w_m$$

die Wurzeln einer Gleichung

$$x^m + c_1 x^{m-1} + c_2 x^{m-2} + \cdots + c_m = 0,$$

und

$$S_k = w_1^k + w_2^k + \cdots + w_m^k,$$

so lauten diese Formeln folgendermaassen:

$$S_1 + c_1 = 0$$
$$S_2 + c_1 S_1 + 2c_2 = 0$$
$$S_3 + c_1 S_2 + c_2 S_1 + 3c_3 = 0$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$S_m + c_1 S_{m-1} + c_2 S_{m-2} + \cdots + c_{m-1} S_1 + m c_m = 0.$$

Aus der Form derselben geht hervor, dass S_1, S_2 . . . S_m ganze rationale Zahlen sein werden, sobald die Coefficienten c_1, c_2 . . . c_m sämmtlich ganze rationale Zahlen sind. Wenden wir dies auf die Gleichung

$$\frac{\Pi\,(x^{\mu_1}-1)}{\Pi\,(x^{\mu_2}-1)}=0$$

an, so ergiebt sich, dass

$$S_k=\Sigma\,\theta^{ak}+\Sigma\,\theta^{bk}$$

für jeden Werth $k=1, 2, 3\ldots$ eine ganze Zahl ist. Andererseits ist nun (Supplemente §. 116)

$$\Sigma\,\theta^{ak}-\Sigma\,\theta^{bk}=\left(\frac{k}{P}\right)i^{1/4(P-1)^2}\sqrt{P},$$

und folglich

$$\Sigma\,\theta^{ak}=\tfrac{1}{2}\left(S_k+\left(\frac{k}{P}\right)i^{1/4(P-1)^2}\sqrt{P}\right)$$

$$\Sigma\,\theta^{bk}=\tfrac{1}{2}\left(S_k-\left(\frac{k}{P}\right)i^{1/4(P-1)^2}\sqrt{P}\right);$$

hiermit sind die Summen der $k$ten Potenzen der Wurzeln von jeder der beiden Gleichungen

$$A(x)=0,\quad B(x)=0$$

gefunden, und da dieselben keine andere Irrationalität enthalten als die Quadratwurzel

$$i^{1/4(P-1)^2}\sqrt{P},$$

so gilt zufolge der Newton'schen Formeln dasselbe von sämmtlichen Coefficienten dieser beiden Gleichungen, und zwar werden zwei gleich hohe Coefficienten in beiden Gleichungen sich nur durch das Vorzeichen dieser Quadratwurzel von einander unterscheiden, d. h. zwei solche Coefficienten werden die Formen

$$y-zi^{1/4(P-1)^2}\sqrt{P}\quad\text{und}\quad y+zi^{1/4(P-1)^2}\sqrt{P}$$

haben, wo y und z rationale Zahlen bedeuten. Man kann ferner behaupten, dass y und z entweder ganze Zahlen oder Brüche mit dem Nenner 2 sind, obgleich dies aus den Newton'schen Formeln nicht unmittelbar hervorgeht; um den Beweis dieser Behauptung anzudeuten, wollen wir jede Gleichung, deren höchster Coefficient $=1$, und deren übrige Coefficienten ganze rationale Zahlen sind, eine primäre Gleichung nennen; dann überzeugt man sich leicht, dass die Summe und Differenz zweier Wurzeln von primären

Gleichungen (und ebenso ihr Product) wieder Wurzeln von primären Gleichungen sind; da nun θ die Wurzel einer primären Gleichung ist, so gilt dasselbe von jedem Coefficienten der Functionen $A(x)$ und $B(x)$ und folglich auch von

$$2y \quad \text{und} \quad 2z i^{\frac{1}{4}(P-1)^2} \sqrt{P},$$

und hieraus folgt sogleich, dass die rationalen Zahlen $2y$ und $2z$ *ganze* Zahlen sein müssen.

Fasst man dies zusammen, so ergiebt sich, dass man gleichzeitig

$$2A(x) = Y(x) - Z(x) i^{\frac{1}{4}(P-1)^2} \sqrt{P}$$
$$2B(x) = Y(x) + Z(x) i^{\frac{1}{4}(P-1)^2} \sqrt{P}$$

setzen kann, wo $Y(x)$ und $Z(x)$ ganze Functionen bedeuten, deren sämmtliche Coefficienten ganze rationale Zahlen sind*). Multiplicirt man die beiden Gleichungen mit einander, so erhält man

$$Y(x)^2 - \left(\frac{-1}{P}\right) P\, Z(x)^2 = 4 \frac{\prod (x^{\mu_1} - 1)}{\prod (x^{\mu_2} - 1)}.$$

§. 140.

Wir bemerken nun noch, dass man immer nur die Hälfte der Coefficienten von $Y(x)$ und $Z(x)$ zu berechnen braucht. Es ist nämlich

$$x^\tau A\left(\frac{1}{x}\right) = \prod (1 - \theta^a x) = (-1)^\tau \theta^{\Sigma a} \prod (x - \theta^{-a})$$

$$x^\tau B\left(\frac{1}{x}\right) = \prod (1 - \theta^b x) = (-1)^\tau \theta^{\Sigma b} \prod (x - \theta^{-b});$$

nun ist, je nachdem $P \equiv 1$, oder $P \equiv 3 \pmod 4$ ist,

$$\left(\frac{-1}{P}\right) = +1, \quad \text{oder} \quad \left(\frac{-1}{P}\right) = -1,$$

und folglich

$$\prod (x - \theta^{-a}) = A(x), \quad \prod (x - \theta^{-b}) = B(x)$$

oder

$$\prod (x - \theta^{-a}) = B(x), \quad \prod (x - \theta^{-b}) = A(x);$$

*) Vergl. *Gauss: D. A.* art. 357.

ist ferner P nicht $= 3$, so existirt unter den Zahlen a eine Zahl a' von der Beschaffenheit, dass $(a'-1)$ relative Primzahl zu P ist, und da die Reste der Producte aa' mit den Zahlen a, und die Reste der Producte ba' mit den Zahlen b im Complex übereinstimmen, so ist

$$a' \Sigma a \equiv \Sigma a, \quad a' \Sigma b \equiv \Sigma b \pmod{P}$$

und folglich

$$\Sigma a \equiv 0, \quad \Sigma b \equiv 0 \pmod{P},$$

also

$$\theta^{\Sigma a} = 1, \quad \theta^{\Sigma b} = 1.$$

Mithin ergiebt sich (da τ gerade, sobald $P \equiv 1 \pmod 4$)

$$\left.\begin{aligned} A(x) &= x^\tau A\left(\frac{1}{x}\right) \\ B(x) &= x^\tau B\left(\frac{1}{x}\right) \end{aligned}\right\}, \text{ wenn } P \equiv 1 \pmod 4$$

und, mit Ausnahme von $P = 3$,

$$\left.\begin{aligned} A(x) &= (-x)^\tau B\left(\frac{1}{x}\right) \\ B(x) &= (-x)^\tau A\left(\frac{1}{x}\right) \end{aligned}\right\}, \text{ wenn } P \equiv 3 \pmod 4$$

und hieraus

$$\left.\begin{aligned} Y(x) &= x^\tau Y\left(\frac{1}{x}\right) \\ Z(x) &= x^\tau Z\left(\frac{1}{x}\right) \end{aligned}\right\}, \text{ wenn } P \equiv 1 \pmod 4$$

und, mit Ausnahme von $P = 3$,

$$\left.\begin{aligned} Y(x) &= (-x)^\tau Y\left(\frac{1}{x}\right) \\ -Z(x) &= (-x)^\tau Z\left(\frac{1}{x}\right) \end{aligned}\right\}, \text{ wenn } P \equiv 3 \pmod 4$$

Diese Gleichungen enthalten Relationen zwischen je zwei gleich weit vom Anfang und Ende abstehenden Coefficienten der Functionen $Y(x)$ und $Z(x)$.

Die wirkliche Berechnung der Coefficienten der beiden Functionen

$$Y(x) = y_0 x^\tau + y_1 x^{\tau-1} + \cdots + y_\tau$$
$$Z(x) = z_0 x^\tau + z_1 x^{\tau-1} + \cdots + z_\tau$$

geschieht nun auf folgende Art. Zuerst bildet man die Potenzsummen

$$S_k = \Sigma\, \theta^{ak} + \Sigma\, \theta^{bk}$$

für $k = 1, 2, 3 \ldots$ bis zu $\frac{1}{2}\tau$ oder $\frac{1}{2}(\tau - 1)$, je nachdem τ gerade oder ungerade ist; dies kann nach dem Obigen dadurch geschehen, dass man ebenso viele Coefficienten der ganzen Function

$$\frac{\Pi\,(x^{\mu_1} - 1)}{\Pi\,(x^{\mu_2} - 1)}$$

vom höchsten an gerechnet durch wirkliche Division bestimmt, und dann die Newton'schen Formeln anwendet; indessen hält es nicht schwer, durch Betrachtungen, welche ebenfalls auf der im §. 138 bewiesenen Haupteigenschaft der Zahlen μ_1 und μ_2 beruhen, folgende Regel abzuleiten: es sei Q der grösste gemeinschaftliche Divisor von k und $P = QR$, und r die Anzahl der in R aufgehenden Primzahlen, so ist*)

$$S_k = (-1)^r \varphi(Q).$$

Nachdem diese Werthe S_k gefunden sind, erhält man die Coefficienten der Functionen $Y(x)$ und $Z(x)$ durch die beiden aus den Newton'schen Formeln abgeleiteten Recursionsgleichungen

$$2k y_k = \left\{ \begin{array}{c} -\left[S_k y_0 + S_{k-1} y_1 + \cdots + S_1 y_{k-1}\right] \\ +\left(\frac{-1}{P}\right) P\left[\left(\frac{k}{P}\right) z_0 + \left(\frac{k-1}{P}\right) z_1 + \cdots + \left(\frac{1}{P}\right) z_{k-1}\right] \end{array} \right\}$$

$$2k z_k = \left\{ \begin{array}{c} +\left[\left(\frac{k}{P}\right) y_0 + \left(\frac{k-1}{P}\right) y_1 + \cdots + \left(\frac{1}{P}\right) y_{k-1}\right] \\ -\left[S_k z_0 + S_{k-1} z_1 + \cdots + S_1 z_{k-1}\right] \end{array} \right\}$$

wenn man noch berücksichtigt, dass

$$y_0 = 2, \quad z_0 = 0$$

ist.

*) Allgemeiner lautet diese Regel so: ist $m = m'P$ eine beliebige positive ganze Zahl, P das Product aus allen von einander verschiedenen in m aufgehenden Primzahlen, und S_k die Summe der $k$ten Potenzen aller primitiven Wurzeln der Gleichung $x^m = 1$, so ist $S_k = 0$, so oft k nicht durch m' theilbar ist; ist aber $k = m'K$, ferner Q der grösste gemeinschaftliche Divisor von K und $P = QR$, und r die Anzahl der in R aufgehenden Primzahlen, so ist

$$S_k = (-1)^r m' \varphi(Q).$$

Beispiel 1: $P = 3$; in diesem Falle müssen alle Coefficienten berechnet werden; da

$$S_1 = -1, \quad \left(\frac{1}{P}\right) = 1$$

ist, so erhält man

$$2y_1 = -S_1 y_0 = 2, \quad 2z_1 = \left(\frac{1}{P}\right) y_0 = 2,$$

und folglich

$$Y(x) = 2x + 1, \quad Z(x) = 1.$$

Beispiel 2: $P = 5$; $\tau = 2$; da wieder

$$S_1 = -1, \quad \left(\frac{1}{P}\right) = 1$$

ist, so erhält man auch wieder

$$y_1 = 1, \quad z_1 =$$

und folglich

$$Y(x) = 2x^2 + x + 2, \quad Z(x) = x.$$

Beispiel 3: $P = 15 = 3.5$; $\tau = 4$; hier ist

$$S_1 = S_2 = 1; \quad \left(\frac{1}{P}\right) = \left(\frac{2}{P}\right) = 1; \quad \left(\frac{-1}{P}\right) = -1;$$

und folglich erhält man successive

$$y_1 = -1, \quad z_1 = 1$$

und

$$y_2 = -4, \quad z_2 = 0;$$

also ist

$$Y(x) = 2x^4 - x^3 - 4x^2 - x + 2, \quad Z(x) = x^3 - x.$$

VIII. Ueber die Pell'sche Gleichung.

§. 141.

Bedeutet D eine positive ganze Zahl, die aber kein vollständiges Quadrat ist, so ist in §. 83 durch die Betrachtung der Perioden von reducirten quadratischen Formen, die zur Determinante D gehören, nachgewiesen, dass die Pell'sche oder Fermat'sche Gleichung

$$t^2 - Du^2 = 1$$

immer unendlich viele Lösungen in ganzen positiven Zahlen t, u besitzt, und es ist dort auch eine Methode gegeben, durch welche alle diese Lösungen gefunden werden können. Es hat durchaus keine Schwierigkeit, den Zusammenhang zwischen allen diesen Lösungen zu finden, sobald nur erst der Hauptpunct bewiesen ist, dass wirklich eine Lösung existirt, in welcher u von Null verschieden ist (§. 85); *Lagrange* gebührt das Verdienst, durch Einführung neuer Principien in die Zahlentheorie diese Schwierigkeit zuerst vollständig überwunden zu haben, und diese Principien sind später in hohem Grade verallgemeinert*). Wir wollen deshalb hier noch einen Beweis der Lösbarkeit der Pell'schen Gleichung

*) Vergl. drei Abhandlungen von *Dirichlet* in den Monatsberichten der Berliner Akademie vom October 1841, April 1842, März 1846; ferner die Comptes rendus der Pariser Akademie 1840, T. X, p. 286—288. — Vergl. *P. Bachmann: De unitatum complexarum theoria.* 1864.

mittheilen, welcher im Wesentlichen auf derselben Grundlage beruht.

Das Fundament dieses Beweises beruht auf der Thatsache, dass immer unendlich viele Paare von ganzen Zahlen x, y existiren, für welche, abgesehen vom Vorzeichen,

$$x^2 - Dy^2 < 1 + 2\sqrt{D}$$

ist; man überzeugt sich hiervon leicht, wenn man aus der Theorie der Kettenbrüche den Satz entlehnt, dass jeder Näherungswerth $x:y$, den man durch Entwicklung einer Grösse ω in einen Kettenbruch erhält, um weniger als y^{-2} von ω verschieden ist; nimmt man also $\omega = \sqrt{D}$, so giebt es, da $\sqrt{D}$ irrational ist, unendlich viele solche Zahlenpaare x, y von der Beschaffenheit, dass, abgesehen vom Vorzeichen,

$$\frac{x}{y} - \sqrt{D} < \frac{1}{y^2}, \text{ also } x - y\sqrt{D} = \frac{\delta}{y}$$

ist, wo δ einen positiven oder negativen echten Bruch bedeutet; hieraus folgt

$$x + y\sqrt{D} = \frac{\delta}{y} + 2y\sqrt{D},$$

und durch Multiplication

$$x^2 - Dy^2 = \frac{\delta^2}{y^2} + 2\delta\sqrt{D} < 1 + 2\sqrt{D}.$$

Um aber Nichts aus der Theorie der Kettenbrüche zu entlehnen, wollen wir diesen Satz noch auf einem andern und zwar ganz einfachen Wege beweisen. Es sei m irgend eine positive ganze Zahl, so legen wir der Zahl y der Reihe nach die $m+1$ Werthe

$$0, 1, 2 \ldots (m-1), m$$

bei, und bestimmen für jeden dieser Werthe die zugehörige ganze Zahl x durch die Bedingung

$$0 \leqq x - y\sqrt{D} < 1,$$

welche offenbar jedesmal durch eine, und nur durch eine ganze Zahl x erfüllt wird. Theilen wir nun das Intervall von 0 bis 1 in m gleiche Intervalle, welche durch die Werthe

$$\frac{0}{m}, \frac{1}{m}, \frac{2}{m} \cdots \frac{m-1}{m}, \frac{m}{m}$$

begrenzt werden, so muss, da die Anzahl $m+1$ der Zahlenpaare x, y grösser ist als die Anzahl m dieser Intervalle, wenigstens eines dieser Intervalle mehr als einen, also mindestens zwei von den Werthen $x - y\sqrt{D}$ enthalten, die zwei *verschiedenen* Werthen von y entsprechen. Wir bezeichnen diese beiden Werthe mit $x' - y'\sqrt{D}$ und $x'' - y''\sqrt{D}$; dann ist, abgesehen vom Vorzeichen, ihr Unterschied

$$(x' - x'') - (y' - y'')\sqrt{D} = x - y\sqrt{D} < \frac{1}{m},$$

und da y', y'' ungleich, nicht negativ und $\leqq m$ sind, so ist (abgesehen vom Vorzeichen) auch $y = y' - y'' \leqq m$ und von Null verschieden; mithin wird $x - y\sqrt{D}$ auch $< y^{-1}$ und von Null verschieden, weil $\sqrt{D}$ irrational ist. Hieraus folgt aber, wie oben, dass

$$x^2 - Dy^2 < 1 + 2\sqrt{D}$$

und von Null verschieden wird.

Dass nun aber auch unendlich viele solche Zahlenpaare x, y existiren, ergiebt sich leicht; sind nämlich schon beliebig viele solche Zahlenpaare x, y gefunden, so kann man immer die ganze Zahl m so gross nehmen, dass m^{-1} kleiner wird als der kleinste der bisher gefundenen Werthe $x - y\sqrt{D}$; für diese Zahl m erhält man aber auf die angegebene Weise wieder ein Zahlenpaar x, y von der Beschaffenheit, dass $x - y\sqrt{D} < m^{-1}$ und folglich auch kleiner als alle früher gefundenen Werthe $x - y\sqrt{D}$ wird, woraus folgt, dass dieses Zahlenpaar x, y von den frühern verschieden ist; mithin ist die Anzahl dieser Zahlenpaare unbegrenzt.

§. 142.

Mit Hülfe dieses Resultates, dass immer unendlich viele Paare von ganzen Zahlen x, y existiren, für welche der absolute Werth von $x^2 - Dy^2 < 1 + 2\sqrt{D}$ und von Null verschieden wird, lässt sich nun leicht beweisen, dass die Gleichung $t^2 - Du^2 = 1$ immer in ganzen Zahlen t, u lösbar ist, und zwar so, dass u von Null verschieden ausfällt.

Da die Anzahl der ganzen Zahlen, welche abgesehen vom Vorzeichen $< 1 + 2\sqrt{D}$ sind, endlich ist, so muss der Ausdruck $x^2 - Dy^2$ für unendlich viele Zahlenpaare x, y einer und derselben (von Null verschiedenen) Zahl k gleich werden; da ferner die Anzahl der verschiedenen Paare von Resten α, β, welche zwei Zahlen $x, y \pmod{k}$ lassen können, endlich, nämlich $= k^2$ ist, so leuchtet ebenso ein, dass mindestens ein solches Restsystem α, β unendlich oft auftreten muss, dass also unter den unendlich vielen Zahlenpaaren x, y, für welche $x^2 - Dy^2 = k$ wird, auch wieder unendlich viele Paare x, y sich finden müssen, in welchen $x \equiv \alpha$, $y \equiv \beta \pmod{k}$ ist, wo α, β zwei bestimmte Reste bedeuten. Sind nun x', y' und x'', y'' irgend zwei solche Zahlenpaare, d. h. ist gleichzeitig

$$x'^2 - Dy'^2 = x''^2 - Dy''^2 = k$$

und

$$x' \equiv x'', \quad y' \equiv y'' \pmod{k},$$

so kann man

$$(x' - y'\sqrt{D})(x'' + y''\sqrt{D}) = k(t + u\sqrt{D})$$

setzen, wo t, u *ganze* Zahlen bedeuten, die offenbar der Gleichung

$$t^2 - Du^2 = 1$$

genügen; und zwar dürfen wir annehmen, dass u von Null verschieden ist; denn aus $u = 0$, $t = \pm 1$ ergiebt sich vermöge der obigen Gleichung $x' - y'\sqrt{D} = \pm (x'' - y''\sqrt{D})$; da aber unendlich viele solche Zahlenpaare x', y' und x'', y'' existiren, so können wir auch immer zwei solche auswählen, dass x'', y'' verschieden von $\pm x', \pm y'$, und folglich u von Null verschieden ausfällt.

Hiermit ist also in der That bewiesen, dass immer eine Lösung t, u der vorstehenden Pell'schen Gleichung existirt, in welcher u von Null verschieden ist.

Hieraus lässt sich dann (wie in §. 85), ebenfalls ohne Hülfe der Theorie der reducirten Formen, zeigen, dass alle Auflösungen t, u sich aus der Gleichung

$$t + u\sqrt{D} = \pm (T + U\sqrt{D})^n$$

ergeben, wo T, U die kleinsten positiven ganzen Zahlen bedeuten, die der Gleichung genügen, und der Exponent n alle positiven und

negativen ganzen Zahlen durchläuft. Nur in der einen Beziehung bleibt diese Theorie der Pell'schen Gleichung unvollständig, dass aus ihr keine directe Methode fliesst, diese kleinste positive Auflösung T, U unmittelbar zu finden. Hierzu und ebenso zur Beurtheilung der Aequivalenz zweier Formen und also auch der Darstellbarkeit einer Zahl durch eine Form bleibt die Theorie der reducirten Formen unentbehrlich.

IX. Ueber die Convergenz und Stetigkeit einiger unendlichen Reihen.

§. 143.

Die von *Abel**) herrührende Methode der theilweisen Summation, welche in §. 101 bei der Untersuchung der Convergenz und Stetigkeit einer unendlichen Reihe angewendet ist, findet gewissermassen ihre Erschöpfung bei dem Beweise des folgenden allgemeinen Satzes, in welchem aus gewissen, von einander unabhängigen Voraussetzungen über zwei Grössenreihen

$$a_1, a_2, a_3 \ldots \quad \text{(a)}$$

$$b_1, b_2, b_3 \ldots \quad \text{(b)}$$

Schlüsse auf die aus ihnen zusammengesetzte Grössenreihe

$$a_1 b_1, a_2 b_2, a_3 b_3 \ldots$$

gezogen werden.

Wenn bei unbegrenzt wachsendem n der Modulus der Summe

$$A_n = a_1 + a_2 + \cdots + a_n$$

endlich bleibt, wenn ferner die aus den Moduln der Differenzen $b_1 - b_2, b_2 - b_3 \ldots$ *gebildete Reihe* $\mathfrak{B}$ *convergirt, und ausserdem* b_n *mit wachsendem n unendlich klein wird; so convergirt die Reihe*

$$\mathfrak{P} = a_1 b_1 + a_2 b_2 + a_3 b_3 + \cdots,$$

und ihr Werth ändert sich stetig mit den Grössen (b), *vorausgesetzt, dass auch* $\mathfrak{B}$ *sich stetig ändert.*

---

*) *Recherches sur la série etc.*, Œuvres complètes. 1839. T. I. p. 66; Crelle's Journal I. p. 311.

Aus der Annahme, dass der Modulus von A_n stets kleiner als eine angebbare Constante H bleibt, und dass die Reihe $\mathfrak{B}$ einen endlichen Werth besitzt, folgt zunächst die unbedingte Convergenz der Reihe

$$\mathfrak{Q} = A_1(b_1 - b_2) + A_2(b_2 - b_3) + \cdots,$$

weil selbst die Moduln ihrer Glieder eine convergente Reihe bilden, deren Summe $< H\mathfrak{B}$ ist. Bezeichnet man nun die Summen der ersten n Glieder der Reihen $\mathfrak{P}$, $\mathfrak{Q}$ resp. mit P_n, Q_n, so ist $P_n = Q_{n-1} + A_n b_n$, und da b_n mit wachsendem n unendlich klein wird, so convergirt auch die Reihe $\mathfrak{P}$, und ihr Werth ist gleich dem der Reihe $\mathfrak{Q}$.

Es genügt daher, den letzten Theil des Satzes für die Reihe $\mathfrak{Q}$ nachzuweisen. Setzt man nun $\mathfrak{Q} = Q_n + \mathfrak{Q}_n$ und $\mathfrak{B} = B_n + \mathfrak{B}_n$, wo B_n die Summe der ersten n Glieder der Reihe $\mathfrak{B}$ bedeutet, so ist der Modul von $\mathfrak{Q}_n < H\mathfrak{B}_n$; bezeichnet man ferner mit $\mathfrak{Q}'$, Q'_n, $\mathfrak{B}'$ ... diejenigen Werthe von $\mathfrak{Q}$, Q_n, $\mathfrak{B}$ ..., welche einem bestimmten System (b′) entsprechen, so wird, wenn die veränderlichen Grössen b_n sich den Grössen b'_n unbegrenzt und zwar der Art annähern, dass $\mathfrak{B}$ sich dem Werthe $\mathfrak{B}'$ nähert, auch $\mathfrak{B}_n$ sich dem Grenzwerthe $\mathfrak{B}'_n$ nähern. Nun kann man, wie klein auch eine gegebene positive Grösse δ sein mag, immer n so gross wählen, dass $H\mathfrak{B}'_n < \delta$ ist; mithin wird im Verlaufe der Annäherung auch $H\mathfrak{B}_n$, und folglich auch der Modul des Restes $\mathfrak{Q}_n$ definitiv $< \delta$ werden, während der erste Bestandtheil Q_n sich seinem Grenzwerthe Q'_n nähert; hieraus folgt, dass der Modul von $\mathfrak{Q} - \mathfrak{Q}'$ schliesslich unter 2δ herabsinkt, dass also $\mathfrak{Q}$ sich dem Grenzwerthe $\mathfrak{Q}'$ nähert, was zu beweisen war*).

Dem vorstehenden Beweise des obigen Satzes fügen wir noch folgende Bemerkungen hinzu. Die Convergenz der Reihe $\mathfrak{Q}$ folgt schon aus den beiden Annahmen, dass A_n endlich bleibt, und dass die Reihe $\mathfrak{B}$ convergirt; zufolge der letzteren muss b_n mit wachsendem n sich einem bestimmten Grenzwerthe $\mathfrak{b}$ nähern, weil ja die aus den Differenzen $b_1 - b_2$, $b_2 - b_3$ ... gebildete Reihe

$$(b_1 - b_2) + (b_2 - b_3) + \cdots = b_1 - \mathfrak{b}$$

*) Offenbar bleibt $\mathfrak{P} = \mathfrak{Q}$ auch dann noch stetig, wenn die oben als constant vorausgesetzten Grössen (a) sich zugleich der Art stetig ändern, dass das Maximum H der Moduln von A_n auch während der Aenderung endlich bleibt.

ebenfalls convergiren muss; aber dieser Grenzwerth $\mathfrak{b}$ kann sehr wohl von Null verschieden sein, und es leuchtet ein, dass in diesem Fall die Reihe $\mathfrak{P}$ stets und nur dann convergirt, wenn A_n mit wachsendem n sich ebenfalls einem bestimmten Grenzwerthe $\mathfrak{A}$ nähert, d. h. wenn die Reihe

$$\mathfrak{A} = a_1 + a_2 + a_3 + \cdots$$

convergirt; und zwar ist dann $\mathfrak{P} = \mathfrak{Q} + \mathfrak{A}\mathfrak{b}$. Durch diese Verschärfung der Annahme über die Constanten (a) wird es also gestattet, die Annahme $\mathfrak{b} = 0$ aufzugeben, während die Annahme, dass $\mathfrak{B}$ einen endlichen Werth besitzt, bestehen bleibt*). Von besonderer Wichtigkeit ist aber die Bemerkung, dass jetzt die Reihe $\mathfrak{P}$ sich schon dann mit den Grössen (b) *stetig* ändert, wenn $\mathfrak{B}$ im Verlaufe der Aenderung *endlich* bleibt, während $\mathfrak{Q}$ mit $\mathfrak{B}$ und $\mathfrak{b}$ auch *unstetig* werden kann. Setzt man nämlich $\mathfrak{A} = A_n + \mathfrak{A}_n$, so wird $a_n = \mathfrak{A}_{n-1} - \mathfrak{A}_n$, und

$$\mathfrak{P} = \mathfrak{A}b_1 - \mathfrak{A}_1(b_1 - b_2) - \mathfrak{A}_2(b_2 - b_3) - \cdots;$$

ist nun δ eine beliebig kleine positive gegebene Grösse, so kann man ν so gross wählen, dass für *alle***) Werthe $n \geqq \nu$ der Modul von $\mathfrak{A}_n < \delta$ wird; während daher die Summe der ersten ν Glieder rechter Hand sich stetig mit den Grössen (b) ändert, bleibt der Modul des Restes $< \delta\mathfrak{B}$ und kann folglich, da $\mathfrak{B}$ endlich bleibt, durch δ so klein gemacht werden, wie man will; mithin ändert sich $\mathfrak{P}$ stetig, was zu beweisen war.

---

*) Die Grössenreihen (b), denen endliche Werthe $\mathfrak{B}$ entsprechen, besitzen unter andern merkwürdigen Eigenschaften die, dass aus je zwei solchen Systemen (b′), (b″) unendlich viele andere abgeleitet werden können, deren allgemeines Glied $c + c'b'_n + c''b''_n$ ist, wo c, c', c'' beliebige, von n unabhängige Grössen bedeuten.

**) Ist das System (a) ebenfalls veränderlich, so ist die Voraussetzung, dass $\mathfrak{A}$ sich stetig mit den Grössen (a) ändert, noch nicht hinreichend für die Stetigkeit von $\mathfrak{P}$, wovon man sich durch die genaue Prüfung des folgenden Beispiels überzeugen wird. Es sei $\psi(x)$ eine stetige Function, welche sowohl für unendlich kleine als auch für unendlich grosse Werthe x unendlich klein wird, wie z. B. $x:(1+x^2)$; ist nun $h \geqq 0$ eine veränderliche Grösse, und $a_n = \psi(nh) - \psi((n-1)h)$, ferner $b_n = 1 - nh$ oder $= 0$, je nachdem $nh < 1$ oder > 1 ist, so nähert sich $\mathfrak{P}$, wenn h unendlich klein wird, nicht dem Werthe Null, welcher $h = 0$ entspricht, sondern dem Werthe

$$\int_0^1 \psi(x)\,dx,$$

obgleich $\mathfrak{A}$ stetig $= 0$, und $\mathfrak{B}$ zwar nicht stetig, aber doch endlich bleibt.

Wir wollen die vorstehenden Principien auf die *Dirichlet'schen Reihen* anwenden; unter dieser Benennung verstehen wir Reihen von folgender Form*)

$$f(s) = \frac{a_1}{k_1^s} + \frac{a_2}{k_2^s} + \frac{a_3}{k_3^s} + \cdots,$$

wo $k_1, k_2\ k_3 \ldots$ positive Constanten von der Art bedeuten, dass $k_n \leqq k_{n+1}$ ist, und dass k_n mit n über alle Grenzen wächst; die Constanten $a_1, a_2, a_3 \ldots$ sind beliebige reelle oder complexe Grössen; ebenso kann die Veränderliche s beliebige reelle oder complexe Werthe annehmen, doch wollen wir uns hier der Einfachheit halber auf *reelle* Werthe s beschränken. Behält A_n die frühere Bedeutung, so ergiebt sich folgender Satz:

Bleibt A_n endlich bei wachsendem n, so convergirt die Reihe $f(s)$ für alle positiven Werthe s und ist nebst ihren sämmtlichen Derivirten stetig; convergirt die Reihe noch für $s = 0$, so ist sie auch an dieser Stelle stetig.

Die Behauptungen über $f(s)$ folgen unmittelbar aus der allgemeinen Untersuchung, wenn man $b_n = k_n^{-s}$ setzt, wodurch $\mathfrak{P}$ in die obige Reihe übergeht; denn $\mathfrak{B}$ ist $= k_1^{-s}$ oder $= 0$, je nachdem $s > 0$ oder $= 0$ ist. Um auch die Endlichkeit und Stetigkeit ihrer Derivirten $f'(s)$ darzuthun, setzen wir, wenn s einen festen positiven Werth, und ε eine sehr kleine positive oder negative Grösse bedeutet,

$$b_n = \frac{1}{\varepsilon}\left(\frac{1}{k_n^s} - \frac{1}{k_n^{s+\varepsilon}}\right),$$

so wird

$$\mathfrak{P} = \frac{f(s) - f(s+\varepsilon)}{\varepsilon}.$$

Wählt man nun ν so gross, dass $s \log k_\nu > 1$, und ε so klein, dass

$$\frac{s}{\varepsilon} \log\left(1 + \frac{\varepsilon}{s}\right) < s \log k_\nu$$

ist, so ist $b_\nu \geqq b_{\nu+1} \geqq b_{\nu+2} \ldots$, weil die Derivirte der Function

$$\frac{1}{\varepsilon}\left(\frac{1}{x^s} - \frac{1}{x^{s+\varepsilon}}\right)$$

*) Sie nehmen die Gestalt von Potenzenreihen an, wenn man $s = -\log x$ setzt.

für alle Werthe $x \geqq k_\nu$ negativ ist; ausserdem ist $\mathfrak{b} = 0$, also $\mathfrak{B}_{\nu-1} = b_\nu$. Wird nun ε unendlich klein, so nähert sich b_n dem Grenzwerthe

$$b'_n = \frac{\log k_n}{k_n^s},$$

und da $b'_\nu \geqq b'_{\nu+1} \geqq b'_{\nu+2} \ldots$, ferner $\mathfrak{b}' = 0$, also $\mathfrak{B}'_{\nu-1} = b'_\nu$ ist, so geht $\mathfrak{B}_{\nu-1}$ stetig in den Grenzwerth $\mathfrak{B}'_{\nu-1}$, und folglich auch $\mathfrak{B}$ stetig in den Werth $\mathfrak{B}'$ über. Mithin nähert sich auch $\mathfrak{P}$ dem Grenzwerthe $\mathfrak{P}'$, d. h. es ist

$$-f'(s) = \frac{a_1 \log k_1}{k_1^s} + \frac{a_2 \log k_2}{k_2^s} + \cdots,$$

und da diese Reihe wieder von derselben Beschaffenheit ist, so wird $f'(s)$ auch eine *stetige* Function von s. Ganz ähnlich lässt sich der Beweis für die Derivirten höherer Ordnung führen.

§. 144.

Der wahre Charakter des zuletzt bewiesenen Satzes besteht darin, dass aus dem Verhalten einer Dirichlet'schen Reihe $f(s)$ für $s = 0$ ein Schluss auf ihr Verhalten für alle positiven Werthe s gezogen wird (man kann ihn leicht so umformen, dass von dem beliebigen Werthe $s = \sigma$ auf alle Werthe $s > \sigma$ geschlossen wird). Unter diesem Gesichtspuncte erscheint von besonderm Interesse eine Vergleichung dieses Satzes mit dem allgemeinen Princip des §. 118; beachtet man nämlich, dass, wenn die dort mit t bezeichnete Grösse zwischen k_n und $k_{n+1} > k_n$ liegt, die entsprechende Grösse $T = n$ nichts Anderes ist, als die Summe der ersten n Glieder der Reihe

$$\frac{1}{k_1^{1+s}} + \frac{1}{k_2^{1+s}} + \frac{1}{k_3^{1+s}} + \cdots$$

für $s = -1$, so erkennt man, dass dort aus dem Verhalten der Reihe für $s = -1$ ein Schluss auf ihr Verhalten für alle positiven Werthe s, und namentlich auf ihr Verhalten an der Stelle $s = 0$ gezogen wird. Eine genauere, auf die Vereinigung und Verallgemeinerung beider Sätze hinzielende Untersuchung führt zu den nachstehenden Resultaten, in welchen zur Abkürzung

$$S_n = \frac{a_1}{k_1^s} + \frac{a_2}{k_2^s} + \cdots + \frac{a_n}{k_n^s}$$

gesetzt ist, während A_n seine frühere Bedeutung behält.

1. *Bleibt $S_n k_n^s$ für einen bestimmten negativen Werth s endlich bei wachsendem n, so gilt Dasselbe für jeden negativen Werth s, und ebenso bleibt $A_n : \log k_n$ endlich.*

2. *Bleibt $A_n : \log k_n$ endlich bei wachsendem n, so convergirt die Reihe $f(s)$ für jeden positiven Werth s.*

3. *Nähern sich $s S_n k_n^s$ und $s S_n k_{n+1}^s$ für einen bestimmten negativen Werth s bei wachsendem n einem gemeinschaftlichen Grenzwerthe $-\omega$, so gilt Dasselbe für jeden negativen Werth s, und ebenso nähern sich $A_n : \log k_n$ und $A_n : \log k_{n+1}$ dem gemeinschaftlichen Grenzwerthe $+\omega$.*

4. *Nähern sich $A_n : \log k_n$ und $A_n : \log k_{n+1}$ bei wachsendem n einem gemeinschaftlichen Grenzwerthe ω, so nähert sich $s f(s)$, wenn s positiv unendlich klein wird, demselben Grenzwerthe ω.*

Offenbar entspringt der Satz des vorigen Paragraphen aus 2., und der Satz des §. 118 aus 3. und 4.; um die Beweise kurz zu führen, bemerken wir, dass, wenn

$$R_n = \frac{a_1}{k_1^r} + \frac{a_2}{k_2^r} + \cdots + \frac{a_n}{k_n^r}$$

gesetzt wird,

$$S_n - R_n k_n^{r-s} = R_1 (k_1^{r-s} - k_2^{r-s}) + \cdots + R_{n-1} (k_{n-1}^{r-s} - k_n^{r-s})$$

ist; zerlegt man die Summe rechter Hand in zwei Bestandtheile, von denen der eine die ersten $(m-1)$ Glieder, der andere die übrigen $(n-m)$ Glieder enthält, und berücksichtigt, dass man allgemein

$$\frac{k_\nu^{r-s} - k_{\nu+1}^{r-s}}{r-s} = \int_{k_{\nu+1}}^{k_\nu} x^{r-s-1} dx = h_\nu^r \int_{k_{\nu+1}}^{k_\nu} x^{-s-1} dx = h_\nu^r \frac{k_{\nu+1}^{-s} - k_\nu^{-s}}{s}$$

setzen kann, wo $k_\nu \leqq h_\nu \leqq k_{\nu+1}$ ist, so erhält man

$$S_n - R_n k_n^{-s} = \frac{r-s}{s} \left\{ M(k_m^{-s} - k_1^{-s}) + N(k_n^{-s} - k_m^{-s}) \right\},$$

wo M und N Mittelwerthe*) aus den Grössen $R_\nu h_\nu^r$ resp. von

*) Unter einem Mittelwerthe aus complexen Grössen z ist jeder complexe Werth ζ von der Beschaffenheit zu verstehen, dass die reellen Bestandtheile von ζ und ζi resp. Mittelwerthe aus den reellen Bestandtheilen der Grössen z und der Grössen zi sind.

$\nu = 1$ bis $\nu = m-1$, und von $\nu = m$ bis $\nu = n-1$ bedeuten. Nimmt man nun, wie im *dritten* Satze an, dass die Grössen $rR_\nu k_\nu^r$, $rR_\nu k_{\nu+1}^r$, also auch die Grössen $rR_\nu h_\nu^r$ mit wachsendem ν sich einem Grenzwerthe $-\omega$ nähern, und lässt man m mit n, doch so langsam über alle Grenzen wachsen, dass $k_m : k_n$ unendlich klein wird, so nähert sich rN dem Grenzwerthe $-\omega$, während M endlich bleibt, und folglich wird, wenn s negativ ist, $sS_n k_n^s$ sich ebenfalls dem Grenzwerthe $-\omega$ nähern. Ist aber $s = 0$, so folgt

$$A_n - R_n k_n^r = r\left\{M\log\left(\frac{k_1}{k_m}\right) + N\log\left(\frac{k_m}{k_n}\right)\right\},$$

und wenn man m der Art mit n über alle Grenzen wachsen lässt, dass $\log k_m : \log k_n$ unendlich klein wird, so ergiebt sich, dass $A_n : \log k_n$ sich dem Werthe $+\omega$ nähert. Die Behauptungen über $sS_n k_{n+1}^s$ und $A_n : \log k_{n+1}$ ergeben sich von selbst, weil aus der Annahme hervorgeht, dass, wenn ω von Null verschieden ist, nothwendig $k_n : k_{n+1}$ sich dem Werthe 1 nähert. Zugleich leuchtet ein, dass der Beweis des *ersten* Satzes auf dieselbe Weise geführt werden kann, und zwar viel einfacher, weil es gar keiner Zerlegung der obigen Summe in zwei Bestandtheile bedarf*).

Der Beweis des *zweiten* und *vierten* Satzes lässt sich in ähnlicher Weise führen; setzt man nämlich, wenn s einen *positiven* Werth hat,

$$K_n = \int_{k_n}^{\infty} \frac{s\log x\,dx}{x^{s+1}} = \frac{1 + s\log k_n}{sk_n^s},$$

so ist

$$K_n - K_{n+1} = \int_{k_n}^{k_{n+1}} \frac{s\log x\,dx}{x^{s+1}} = \log h_n (k_n^{-s} - k_{n+1}^{-s});$$

nimmt man daher an, dass $A_n : \log k_n$ endlich bleibt, so folgt hieraus leicht**), dass die unendliche Reihe

---

*) Die auf den ersten Blick auffallende Erscheinung, dass der obige Beweis auch für positive Werthe r gilt, hängt mit ähnlichen Sätzen über das Verschwinden von $f(s) - S_n$ für positive Werthe s bei wachsendem n zusammen.

**) Offenbar darf man, ohne die Allgemeinheit der Sätze zu beeinträchtigen, bei ihrem Beweise annehmen, dass schon $k_1 > 1$ ist.

$$A_1(k_1^{-s} - k_2^{-s}) + A_2(k_2^{-s} - k_3^{-s}) + \cdots$$
$$= \frac{A_1}{\log h_1}(K_1 - K_2) + \frac{A_2}{\log h_2}(K_2 - K_3) + \cdots$$

convergirt, und dass ihre Summe mit $f(s)$ übereinstimmt, womit der zweite Satz bewiesen ist. Bezeichnet man ferner mit M und M' Mittelwerthe aus den Grössen $A_n : \log h_n$ resp. von $n = 1$ bis $n = m - 1$, und von $n = m$ bis $n = \infty$, so kann man

$$f(s) = M(K_1 - K_m) + M' K_m$$

setzen; nimmt man nun (wie im vierten Satze) an, dass die Grössen $A_n : \log k_n$ und $A_n : \log k_{n+1}$ sich einem gemeinschaftlichen Grenzwerthe ω nähern, so gilt Dasselbe von $A_n : \log h_n$; lässt man daher, während s positiv unendlich klein wird, gleichzeitig m über alle Grenzen, doch so langsam wachsen, dass $s \log k_m$ unendlich klein wird, so nähert sich M' dem Grenzwerthe ω, während M endlich bleibt, und da sK_1 und sK_m sich dem gemeinschaftlichen Grenzwerthe 1 nähern, so nähert sich $sf(s)$ dem Grenzwerthe ω, was zu beweisen war.

Nachdem die obigen Sätze bewiesen sind, führen wir einige Beispiele an, hauptsächlich um zu zeigen, dass sie nicht ohne Weiteres umgekehrt werden dürfen.

Beispiel 1. Ist $c > 1$, und $s > 0$, so ist

$$f(s) = \frac{a}{c^s} + \frac{b}{c^{2s}} + \frac{a}{c^{3s}} + \frac{b}{c^{4s}} + \cdots = \frac{ac^s + b}{c^{2s} - 1};$$

für jeden negativen Werth s ist bei wachsendem n

$$\lim S_{2n} c^{2ns} = \frac{ac^s + b}{1 - c^{2s}}, \quad \lim S_{2n+1} c^{(2n+1)s} = \frac{a + bc^s}{1 - c^{2s}},$$

also schwankt $S_n k_n^s$, und nur, wenn $b = a$ ist, wird

$$\lim S_n k_n^s = \frac{a}{1 - c^s};$$

trotzdem ist, auch wenn a und b ungleich sind,

$$\lim \frac{A_n}{\log k_n} = \lim \frac{A_n}{\log k_{n+1}} = \frac{a + b}{2 \log c},$$

und wirklich nähert sich $sf(s)$ für unendlich kleine positive Werthe von s demselben Grenzwerth.

Beispiel 2. Ist wieder $c > 1$, und $s > 0$, so ist

$$f(s) = \frac{1}{c^s} - \frac{2}{c^{2s}} + \frac{3}{c^{3s}} - \frac{4}{c^{4s}} + \cdots = \frac{c^s}{(c^s+1)^2};$$

da $A_{2n} = -n$, $A_{2n-1} = +n$ ist, so schwankt $A_n : \log k_n$; dennoch nähert sich $sf(s)$ dem bestimmten Grenzwerth Null, wenn s positiv unendlich klein wird.

Beispiel 3. Von grösserem Interesse ist die folgende Reihe

$$f(s) = e^{-s} + ce^{-sc} + c^2e^{-sc^2} + c^3e^{-sc^3} + \cdots,$$

wo c wieder >1 ist; da $\log k_n = c^{n-1}$, und

$$A_n = 1 + c + c^2 + \cdots + c^{n-1} = \frac{c^n - 1}{c - 1},$$

so ergiebt sich bei wachsendem n

$$\lim \frac{A_n}{\log k_n} = \frac{c}{c-1}, \quad \lim \frac{A_n}{\log k_{n+1}} = \frac{1}{c-1},$$

und es zeigt sich, dass $sf(s)$ für unendlich kleine positive Werthe von s sich keinem Grenzwerthe nähert, sondern hin- und herschwankt. Ist nämlich r ein bestimmter positiver Werth, und lässt man $s = rc^{-\varrho}$ dadurch unendlich klein werden, dass ϱ wachsend alle positiven ganzen Zahlen durchläuft, so nähert sich $sf(s)$ dem bestimmten, aber von r abhängigen Grenzwerth

$$\psi(r) = \Sigma\, r c^n e^{-rc^n},$$

wo n alle ganzen Zahlen von $-\infty$ bis $+\infty$ durchlaufen muss. Offenbar ist $\psi(r)$ eine periodische Function von $\log r$, welche sich in die Fourier'sche Reihe

$$\frac{1}{\log c} \Sigma\, z^n \Pi\left(\frac{2n\pi i}{\log c}\right)$$

verwandeln lässt, wo $\log z \log c = -2\pi i \log r$ ist, Π das Euler'sche Integral zweiter Art bedeutet, und n alle ganzen Zahlen von $-\infty$ bis $+\infty$ durchläuft; sie convergirt für jeden complexen Werth r, dessen reeller Bestandtheil positiv ist; sie ist zugleich der Grenzwerth des Integrals

$$\int_{-\infty}^{+\infty} r c^x e^{-rc^x} dx \cdot \frac{\sin(2n+1)\pi x}{\sin \pi x}$$

für unendlich grosse Werthe der positiven ganzen Zahl n. Wird s stetig positiv unendlich klein, so schwankt $sf(s)$ um den mittlern Werth $1 : \log c$, welcher auch zwischen den Grenzwerthen von $A_n : \log k_n$ und $A_n : \log k_{n+1}$ liegt.

X. Ueber die Composition der binären quadratischen Formen.

§. 145.

Den Ausgangspunct für unsere Darstellung der von *Gauss**) gegründeten Theorie der Composition bildet folgendes Lemma:

Ist

$$bb \equiv D \pmod{a}, \quad b'b' \equiv D \pmod{a'}, \tag{1}$$

und haben die drei Zahlen $a, a', b+b'$ *keinen gemeinschaftlichen Theiler, so existirt in Bezug auf den Modulus* aa' *eine und nur eine Classe von Zahlen* B*, welche den drei Bedingungen*

$$B \equiv b \pmod{a}, \quad B \equiv b' \pmod{a'}, \quad BB \equiv D \pmod{aa'} \tag{2}$$

genügen.

Dies leuchtet unmittelbar ein, falls a und a' relative Primzahlen sind (§§. 25, 37); unter der allgemeineren Voraussetzung aber, dass $a, a', b+b'$ keinen gemeinschaftlichen Theiler haben, bestimme man (nach §. 24) drei ganze Zahlen h, h', h'', welche die Bedingung

$$ha + h'a' + h''(b+b') = 1 \tag{3}$$

befriedigen; dann werden alle durch die Congruenz

$$B \equiv hab' + h'a'b + h''(bb' + D) \pmod{aa'} \tag{4}$$

bestimmten Zahlen B und nur diese den Forderungen (2) genügen. Da nämlich

---

*) *D. A.* art. 234 seqq. — Vergl. *Lejeune Dirichlet: De formarum binariarum secundi gradus compositione.* 1851.

$$(B-b)(B-b') = BB-(b+b')B+bb'$$

ist, so folgt zunächst, dass die Forderungen (2) vollständig übereinstimmen mit den folgenden

$$a'B \equiv a'b,\ aB \equiv ab',\ (b+b')B \equiv bb'+D \pmod{aa'}, \quad (5)$$

welche, mit h', h, h'' multiplicirt und addirt, die Congruenz (4) nach sich ziehen. Dass umgekehrt jede durch die Congruenz (4) bestimmte Zahl B den Bedingungen (2) oder (5) genügt, ergiebt sich leicht, wenn man aus (3) und (4) der Reihe nach h', h, h'' eliminirt und hierbei die Voraussetzungen (1) berücksichtigt.

Wir bemerken schliesslich, dass die Zahlen a, a', $2B$ keinen gemeinschaftlichen Theiler haben; denn ist δ ein solcher, so folgt aus (2) auch $b \equiv b' \equiv B \pmod{\delta}$, also $b+b' \equiv 2B \equiv 0 \pmod{\delta}$; mithin ist δ gemeinschaftlicher Theiler von a, a', $b+b'$, und folglich $\delta = 1$.

§. 146.

Zwei binäre quadratische Formen (a, b, c), (a', b', c') von gleicher Determinante D sollen *einig**) heissen, wenn die Zahlen a, a', $b+b'$ keinen gemeinschaftlichen Theiler haben. Da unter dieser Voraussetzung auch $bb \equiv D \pmod{a}$, $b'b' \equiv D \pmod{a'}$ ist, so folgt aus dem vorhergehenden Lemma unmittelbar die Existenz von unendlich vielen (nach §. 56 äquivalenten) Formen (aa', B, C) derselben Determinante D, deren mittlere Coefficienten B den Bedingungen $B \equiv b \pmod{a}$, $B \equiv b' \pmod{a'}$ genügen; jede solche Form (aa', B, C) heisse *zusammengesetzt***) (*composita*) *aus* (a, b, c) *und* (a', b', c').

Wir bemerken zunächst, dass (nach §. 56) die Formen (a, b, c), (a', b', c') resp. den Formen $(a, B, a'C)$, (a', B, aC) äquivalent sind; diese letzteren sind ebenfalls einig, weil die Zahlen a, a', $2B$, keinen gemeinschaftlichen Theiler haben (§. 145), und aus ihnen ist ebenfalls die Form (aa', B, C) zusammengesetzt. Bedeuten nun x, y, x', y' variabele Grössen, und setzt man

*) Diese Benennung soll an die *radices concordantes* von *Dirichlet* erinnern.

**) Vergl. *Gauss*: *D. A.* artt. 235, 212, 243, 244.

$$X = xx' - Cyy', \quad Y = (ax + By)\,y' + (a'x' + By')\,y, \qquad (1)$$

so wird

$$(ax + (B + \sqrt{D})y)(a'x' + (B + \sqrt{D})y') = aa'X + (B + \sqrt{D})\,Y; \qquad (2)$$

ersetzt man hierin $\sqrt{D}$ durch $-\sqrt{D}$ und multiplicirt die so entstehende Gleichung mit der vorstehenden, so ergiebt sich nach Wegwerfung des beiden Seiten gemeinschaftlichen Factors aa' die Gleichung

$$\begin{aligned}(ax^2 + 2Bxy + a'Cy^2)\,(a'x'^2 + 2Bx'y' + aCy'^2)\\ = aa'X^2 + 2BXY + CY^2,\end{aligned} \qquad (3)$$

d. h. *die Form (aa', B, C) geht durch die bilineare Substitution* (1) *in das Product aus den beiden Formen $(a, B, a'C)$, (a', B, aC) über.*

Auf dem vorstehenden Resultate beruht zugleich der Beweis des folgenden Fundamentalsatzes*):

Sind die beiden einigen Formen (a, b, c), (a', b', c') resp. äquivalent den beiden einigen Formen (m, n, l), (m', n', l'), so ist auch die aus den beiden ersteren zusammengesetzte Form (aa', B, C) äquivalent der aus den beiden letzteren zusammengesetzten Form (mm', N, L).

Aus den Voraussetzungen folgt zunächst, dass die Formen $(a, B, a'C)$, (a', B, aC) resp. den Formen $(m, N, m'L)$, (m', N, mL) äquivalent sind, und hieraus (nach §. 60. Anmerkung) die Existenz von vier ganzen Zahlen x, y, x', y', welche den folgenden Bedingungen genügen

$$ax^2 + 2Bxy + a'Cy^2 = m, \quad a'x'^2 + 2Bx'y' + aCy'^2 = m' \qquad (4)$$

$$ax + (B + N)y \equiv 0, \quad (B - N)x + a'Cy \equiv 0 \pmod{m} \qquad (5)$$

$$a'x' + (B + N)y' \equiv 0, \quad (B - N)x' + aCy' \equiv 0 \pmod{m'}, \qquad (6)$$

und ebenso braucht man, um die Aequivalenz der beiden Formen (aa', B, C), (mm', N, L) darzuthun, nur die Existenz von zwei ganzen Zahlen X, Y nachzuweisen, welche die Forderungen

$$aa'X^2 + 2BXY + CY^2 = mm' \qquad (7)$$

$$aa'X + (B + N)Y \equiv 0 \pmod{mm'} \qquad (8)$$

$$(B - N)X + CY \equiv 0 \pmod{mm'} \qquad (9)$$

befriedigen. Es lässt sich nun leicht zeigen, dass die beiden (offenbar ganzen) Zahlen X, Y, welche nach (1) aus den vier ganzen

*) *Gauss: D. A.* art. 239. — *Dirichlet* a. a. O.

Zahlen x, y, x', y' gebildet sind, in der That den vorstehenden Bedingungen genügen. Zunächst folgt (7) unmittelbar aus (3) und (4). Da ferner aus jeder Gleichung von der Form

$$(t+u\sqrt{D})\,(t'+u'\sqrt{D}) = (t''+u''\sqrt{D})\,(t'''+u'''\sqrt{D}),$$

wo t, u, t' u. s. w. ganze Zahlen bedeuten, die in Bezug auf die Variabele z identische Gleichung

$$(t+uz)\,(t'+u'z) = (t''+u''z)\,(t'''+u'''z) + (uu'-u''u''')\,(zz-D),$$

und hieraus, da $NN \equiv D \pmod{mm'}$ ist, auch die Congruenz

$$(t+uN)\,(t'+u'N) \equiv (t''+u''N)\,(t'''+u'''N) \pmod{mm'}$$

hervorgeht, so folgt (8) unmittelbar aus (2) unter Berücksichtigung von (5) und (6). Dieselbe Gleichung (2) lässt sich endlich durch Multiplication mit $B-\sqrt{D}$, oder mit C, und durch Division mit a oder mit a' auf die folgenden vier Formen bringen

$$((B-\sqrt{D})x+a'Cy)\,(a'x'+(B+\sqrt{D})y') = a'U$$
$$(ax+(B+\sqrt{D})y)\,((B-\sqrt{D})x'+aCy') = aU$$
$$((B-\sqrt{D})x+a'Cy)\,((B-\sqrt{D})x'+aCy') = (B-\sqrt{D})U$$
$$C(ax+(B+\sqrt{D})y)\,(a'x'+(B+\sqrt{D})y') = (B+\sqrt{D})U,$$

wo zur Abkürzung

$$(B-\sqrt{D})X+CY = U$$

gesetzt ist; ersetzt man überall $\sqrt{D}$ durch N, so gehen nach dem oben angeführten Princip diese Gleichungen wieder in Congruenzen nach dem Modulus mm' über; bezeichnet man den aus U hervorgehenden Ausdruck, d. h. die linke Seite der zu beweisenden Congruenz (9), mit V, so ergiebt sich unter Berücksichtigung von (5) und (6), dass die Producte $a'V$, aV, $(B-N)V$, $(B+N)V$, mithin auch $2BV$ durch mm' theilbar sind; da aber die Factoren a, a', $2B$ keinen gemeinschaftlichen Theiler haben, so muss der andere Factor V für sich allein durch mm' theilbar sein, also die Congruenz (9) wirklich Statt finden.

Mithin genügen die beiden ganzen Zahlen X, Y den Bedingungen (7), (8), (9), und hieraus folgt (nach §. 60. Anmerkung) die Aequivalenz der Formen (aa', B, C), (mm', N, L); was zu beweisen war.

§. 147.

Um den Charakter des eben bewiesenen Fundamentalsatzes in das rechte Licht zu setzen, bemerken wir zunächst Folgendes: *Sind* (a, b, c), (a', b', c') *zwei einige Formen, so sind ihre Theiler* σ, σ' (§. 61) *relative Primzahlen, und* $\sigma\sigma'$ *ist der Theiler der aus ihnen zusammengesetzten Form* (aa', B, C). Denn da die Formen (a, b, c), (a', b', c') resp. den Formen $(a, B, a'C)$, (a', B, aC) äquivalent sind, so ist (nach §. 61) σ der grösste gemeinschaftliche Divisor von $a, 2B, a'C$, und σ' ist der grösste gemeinschaftliche Divisor von $a', 2B, aC$; da nun $a, a', 2B$ keinen gemeinschaftlichen Divisor haben, so muss die in a und $2B$ aufgehende Zahl σ relative Primzahl zu a' (und also auch zu der in a' aufgehenden Zahl σ') sein; und da σ in $a'C$ aufgeht, so muss σ auch in C aufgehen; ebenso muss σ' relative Primzahl zu a sein und folglich auch in C aufgehen. Da ferner schon gezeigt ist, dass σ und σ' relative Primzahlen sind, und da beide sowohl in $2B$, als auch in C aufgehen, so ist $\sigma\sigma'$ offenbar gemeinschaftlicher Divisor der drei Zahlen aa', $2B$, C. Wollte man nun annehmen, $\sigma\sigma'$ wäre nicht ihr grösster gemeinschaftlicher Divisor, sondern sie liessen sich nach der Division mit $\sigma\sigma'$ noch durch eine Primzahl p theilen, so müsste p wenigstens in einer der beiden Zahlen $a:\sigma$ oder $a':\sigma'$ aufgehen; gesetzt aber, p ginge in $a:\sigma$ auf, so hätten die drei Zahlen $a, 2B, a'C$ den gemeinschaftlichen Divisor $p\sigma$, während doch σ ihr grösster gemeinschaftlicher Divisor ist. Ebenso wenig kann p in $a':\sigma'$ aufgehen, und folglich ist $\sigma\sigma'$ der grösste gemeinschaftliche Divisor der Zahlen aa', $2B$, C, d. h. $\sigma\sigma'$ ist der Theiler der Form (aa', B, C), was zu beweisen war.

Umgekehrt: *hat man zwei Formenclassen* K, K' *von gleicher Determinante* D, *deren Theiler* σ, σ' *relative Primzahlen sind, so kann man stets zwei einige Formen* (a, b, c), (a', b', c') *resp. aus den Classen* K, K' *auswählen.* Denn man kann (nach §. 93) den Repräsentanten (a, b, c) der Classe K zunächst so wählen, dass a relative Primzahl zu σ' wird, worauf der Repräsentant (a', b', c') der Classe K' so gewählt werden kann, dass a' relative Primzahl zu a wird; dann sind aber (a, b, c), (a', b', c') gewiss zwei einige Formen. Wie nun auch zwei einige Formen aus den Classen K, K'

ausgewählt sein mögen, so wird zufolge des bewiesenen Fundamentalsatzes die aus ihnen zusammengesetzte Form stets einer und derselben Formenclasse $\mathfrak{K}$ von derselben Determinante D angehören, deren Theiler nach dem Obigen $= \sigma\sigma'$ ist. Wir werden daher sagen, dass diese *Classe* $\mathfrak{K}$ *aus den beiden einigen Classen* K, K' *zusammengesetzt* ist, und werden dies durch die symbolische Gleichung*)

$$\mathfrak{K} = KK' = K'K$$

ausdrücken.

Sind ferner je zwei der drei Classen K, K', K'' einig, so lassen sie sich successive zu einer Classe zusammensetzen, und zwar wird diese resultirende Classe von der Anordnung der beiden successiven Compositionen völlig unabhängig sein**); d. h. symbolisch ausgedrückt, es wird

$$(KK')K'' = (KK'')K' = (K'K'')K$$

sein. Man kann nämlich die Repräsentanten (a, b, c), (a', b', c'), (a'', b'', c'') der drei Classen K, K', K'' (nach §. 93) so wählen, dass a, a', a'' relative Primzahlen sind; bestimmt man nun (nach §. 25) B durch die Congruenzen

$$B \equiv b \pmod{a},\ B \equiv b' \pmod{a'},\ B \equiv b'' \pmod{a''},$$

so wird von selbst $BB \equiv D \pmod{aa'a''}$, also $D = BB - aa'a''C$, wo C eine ganze Zahl bedeutet. Dann enthält

die Classe	K	die Form	$(a, B, a'a''C)$
„ „	K'	„ „	$(a', B, aa''C)$
„ „	K''	„ „	$(a'', B, aa'C)$
„ „	KK'	„ „	$(aa', B, a''C)$
„ „	KK''	„ „	$(aa'', B, a'C)$
„ „	$K'K''$	„ „	$(a'a'', B, aC)$

und jede der Classen $(KK')K''$, $(KK'')K'$, $(K'K'')K$ enthält folglich dieselbe Form $(aa'a'', B, C)$; mithin sind diese drei Classen identisch. Diese eine Classe kann daher einfach durch das Symbol $KK'K''$ bezeichnet werden, wobei die Stellung der drei Symbole K, K', K'' gleichgültig ist.

Wendet man nun dieselbe Schlussfolgerung an, wie in §. 2, so ergiebt sich, dass auch für jede grössere Anzahl von Classen

*) *Gauss* bezeichnet die aus K und K' zusammengesetzte Classe mit $K + K'$ (*D. A.* art. 249).

**) *Gauss: D. A.* artt. 240, 241.

$K, K' \ldots$ die durch ihre successive Composition entstehende Classe völlig bestimmt, und von der Anordnung der Composition gänzlich unabhängig ist. Erforderlich bleibt aber die Bedingung, dass diese Classen $K, K' \ldots$ zu derselben Determinante gehören, und dass ihre Theiler $\sigma, \sigma' \ldots$ relative Primzahlen sind, weil nur dann die Composition in der oben angegebenen Art ausgeführt werden kann; für unsere Zwecke reicht aber dieser specielle Fall der allgemeineren Theorie der Composition völlig aus.

§. 148.

Wir betrachten zunächst einige besonders wichtige specielle Fälle der Classencomposition *).

1. Die Hauptform $(1, 0, -D)$ ist offenbar einig mit jeder Form (a, b, c) derselben Determinante, und die Composition beider Formen giebt als Resultat dieselbe Form (a, b, c), also: *Durch Composition irgend einer Classe K mit der Hauptclasse entsteht immer die Classe K.* Bezeichnet man daher die Hauptclasse durch das Symbol 1, so ist immer $1\,K = K$, wo K eine beliebige Classe bedeutet.

2. Ist (a, b, c) eine ursprüngliche Form der ersten Art, so ist sie einig mit der Form (c, b, a), und aus beiden ist die Form $(ac, b, 1)$ zusammengesetzt. Da nun (c, b, a) mit $(a, -b, c)$, und ebenso $(ac, b, 1)$ mit $(1, -b, ac)$ und folglich auch mit der Hauptform $(1, 0, -D)$ äquivalent ist (§. 56), so kann man dies Resultat kurz so aussprechen: *Die Composition von zwei entgegengesetzten ursprünglichen Classen der ersten Art H, H' giebt stets die Hauptclasse $HH' = 1$.*

Hieraus ziehen wir eine wichtige Folgerung, von welcher sehr häufig Gebrauch gemacht wird: *Bedeutet H eine ursprüngliche Classe erster Art, so folgt aus $HK = HL$ auch stets $K = L$.* Ist nämlich H' der Classe H entgegengesetzt, also $HH' = 1$, so folgt aus $HK = HL$ zunächst $(HK)H' = (HL)H'$, und hieraus $(HH')K = (HH')L$, also $K = L$.

*) *Gauss: D. A.* artt. 243, 250.

3. Ist K eine Classe vom Theiler σ, so kann man (nach §. 93) ihren Repräsentanten $(a\sigma, b, c)$ so wählen, dass a relative Primzahl zu σ ist; dann ist diese Form offenbar zusammengesetzt aus den beiden einigen Formen $(a, b, c\sigma)$ und (σ, b, ac), deren letztere den Theiler σ hat und der einfachsten Classe dieses Theilers angehört (§. 61), woraus von selbst folgt, dass die erstere Form eine ursprüngliche Form der ersten Art sein muss, was sich auch leicht direct nachweisen liesse. Wir haben daher das Resultat: *Ist S die einfachste, und K irgend eine Classe vom Theiler σ, so giebt es immer mindestens eine ursprüngliche Classe erster Art H von der Beschaffenheit, dass $SH = K$ ist.*

Man überzeugt sich leicht mit Hülfe von 2., dass der Satz 3. auch dann noch gilt, wenn S und K irgend welche Classen desselben Theilers bedeuten; ebenso leuchtet ein, dass aus den einfachsten Classen der Theiler σ, σ' stets die einfachste Classe des Theilers $\sigma\sigma'$ zusammengesetzt ist, natürlich unter der Voraussetzung, dass σ und σ' relative Primzahlen sind. Wir verweilen aber nicht länger bei diesen und anderen ebenso leicht zu beweisenden Sätzen, weil sie für die nachfolgenden Untersuchungen völlig entbehrlich sind.

§. 149.

Durch Composition einer *ursprünglichen Classe der ersten Art A* mit sich selbst, oder kürzer, durch *Duplication**) der Classe A entsteht eine Classe AA, welche man auch durch A^2 bezeichnen kann; ähnlich ist die allgemeine Bezeichnung A^m zu verstehen, wo m irgend eine positive ganze Zahl bedeutet. Durch Anwendung derselben Schlüsse, wie in §. 28, findet man nun leicht, dass immer ein kleinster positiver Exponent δ existirt, welcher der Bedingung $A^\delta = 1$ genügt; dann sind die Classen

$$1, A, A^2 \ldots A^{\delta-1},$$

welche die sogenannte *Periode***) der Classe A bilden, von einander verschieden; aus $A^r = A^s$ folgt $r \equiv s \pmod{\delta}$, und umgekehrt; verallgemeinert man hiernach die Bezeichnung A^m, in-

*) *Gauss: D. A.* art. 249.
**) *Gauss: D. A.* art. 306. II.

dem man sie auch auf negative Exponenten m (und auf $m = 0$) ausdehnt, so ist z. B. $A^{-1} = A^{\vartheta-1}$ das Symbol für die Classe, welche der Classe A entgegengesetzt ist (§. 148, 2.).

Eine solche Classenperiode bildet nur einen speciellen Fall des folgenden neuen Begriffs, welcher von der höchsten Wichtigkeit für die Gesetze der Composition ist: Ein System $\mathfrak{A}$ von ursprünglichen Classen der ersten Art soll eine *Gruppe**) heissen, wenn die Composition von je zwei Classen des Systems $\mathfrak{A}$ immer wieder eine Classe desselben Systems liefert; die Anzahl a der in $\mathfrak{A}$ enthaltenen verschiedenen Classen heisse der *Grad* dieser Gruppe $\mathfrak{A}$.

Aus dieser Erklärung folgt sofort, dass, wenn die Classe A in einer Gruppe $\mathfrak{A}$ enthalten ist, auch die ganze Periode der Classe A, also auch die entgegengesetzte Classe A^{-1} und die Hauptclasse sich in $\mathfrak{A}$ vorfindet. Setzt man ferner jede in der Gruppe $\mathfrak{A}$ enthaltene Classe A_1, $A_2 \ldots A_a$ mit einer ursprünglichen Classe erster Art B zusammen, so sind die entstehenden Classen $A_1 B$, $A_2 B \ldots A_a B$ von einander verschieden (§. 148, 2.) und bilden einen Complex, den wir kurz durch $\mathfrak{A}B$ bezeichnen können; zwei so gebildete Complexe $\mathfrak{A}B$ und $\mathfrak{A}B'$ sind nun entweder vollständig identisch (was wieder durch das Zeichen $=$ angedeutet werden soll), oder sie haben keine einzige gemeinschaftliche Classe; denn wenn sie eine gemeinschaftliche Classe $AB = A'B'$ haben, wo A und A' in $\mathfrak{A}$ enthalten sind, so folgt $B = A^{-1}A'B' = A''B'$, wo $A'' = A^{-1}A'$ eine ebenfalls in $\mathfrak{A}$ enthaltene Classe bedeutet, und hieraus $\mathfrak{A}B = \mathfrak{A}A''B' = \mathfrak{A}B'$, weil offenbar der Complex $\mathfrak{A}A''$ mit $\mathfrak{A}$ selbst identisch ist.

Stützt man sich auf diese fundamentale Eigenschaft einer Gruppe und wendet dieselbe Schlussfolgerung an, wie in §. 127, so ergiebt sich unmittelbar folgender Satz:

Sind alle a Classen einer Gruppe $\mathfrak{A}$ zugleich in einer Gruppe $\mathfrak{B}$ vom Grade b enthalten, so ist a ein Divisor von $b = \mu a$, und die Gruppe $\mathfrak{B}$ besteht aus μ Complexen von der Form $\mathfrak{A}B$; die Gruppe $\mathfrak{A}$ soll daher auch ein *Divisor* der Gruppe $\mathfrak{B}$, letztere ein *Multiplum* der ersteren heissen.

---

*) Ich wähle absichtlich diese von *Galois* in die Algebra eingeführte Benennung, weil seine Theorie und die obige, welche den sogenannten Abel'schen Gleichungen entspricht, gemeinschaftlich enthalten sind in der allgemeineren Theorie der Composition, in welcher $(KK')K'' = K(K'K'')$ ist, und ausserdem sowohl aus $KK' = KK''$, als auch aus $K'K = K''K$ stets $K' = K''$ folgt (vergl. §. 85).

Sind ferner $\mathfrak{A}$ und $\mathfrak{B}$ zwei beliebige Gruppen, so bildet das System $\mathfrak{D}$ aller in $\mathfrak{A}$ und $\mathfrak{B}$ gemeinschaftlich enthaltenen Classen ebenfalls eine Gruppe, welche der grösste gemeinschaftliche Divisor von $\mathfrak{A}$ und $\mathfrak{B}$ heissen mag; sind a, b, d die Grade dieser drei Gruppen, so ist d ein gemeinschaftlicher Divisor von $a = \alpha d$ und $b = \beta d$; besteht ferner die Gruppe $\mathfrak{B}$ aus den β Complexen $\mathfrak{D}B_1$, $\mathfrak{D}B_2 \ldots \mathfrak{D}B_\beta$, so bilden, wie man leicht erkennt, auch die β Complexe $\mathfrak{A}B_1$, $\mathfrak{A}B_2 \ldots \mathfrak{A}B_\beta$ eine Gruppe $\mathfrak{M}$ vom Grade $m = a\beta = b\alpha = ab : d$, und zwar ist diese Gruppe $\mathfrak{M}$ das kleinste gemeinschaftliche Multiplum der beiden Gruppen $\mathfrak{A}$ und $\mathfrak{B}$ *).

Die am leichtesten zu überblickenden Gruppen sind die oben erwähnten Perioden; jede solche Gruppe, deren Classen durch wiederholte Composition aus einer einzigen Classe entstehen, wollen wir eine *reguläre* Gruppe nennen; jede *irreguläre* Gruppe lässt sich als das kleinste Multiplum von gewissen regulären Gruppen darstellen, von denen je zwei nur die Hauptclasse gemeinschaftlich haben. Auf diese Darstellung und die damit zusammenhängenden Sätze von *Gauss* **), deren Beweis leicht auf das Vorhergehende gegründet werden kann, wollen wir aber hier nicht mehr eingehen.

§. 150.

Eine der hauptsächlichsten Anwendungen, welche *Gauss* von der Theorie der Composition gemacht hat, besteht in der Vergleichung der Anzahl h' der Classen vom Theiler σ mit der Anzahl h der ursprünglichen Classen erster Art ***); offenbar ist dies dieselbe Aufgabe, welche Dirichlet in der oben mitgetheilten Art (§§. 97, 99, 100) gelöst hat.

Bedeutet S die einfachste, und K irgend eine Classe vom Theiler σ, so existirt (nach §. 148, 3.) *mindestens* eine ursprüngliche Classe erster Art H, welche mit S componirt die Classe K

*) Dieser Satz verliert seine allgemeine Gültigkeit, wenn die *Ordnung* der zusammenzusetzenden Elemente einen Einfluss auf das Compositum hat.

**) *D. A.* artt. 305 — 307; ferner *Démonstration de quelques théorèmes concernants les périodes des classes des formes binaires du second degré* (Gauss Werke, Bd. II. p. 266. 1863). — Vergl. *Schering: Die Fundamental-Classen der zusammensetzbaren arithmetischen Formen.* Göttingen 1869.

***) *D. A.* artt. 253 — 256.

hervorbringt; durch Composition von S mit allen h Classen H müssen also jedenfalls alle Classen K vom Theiler σ, jede mindestens einmal erzeugt werden. Es seien nun $R_1, R_2 \ldots R_r$ die sämmtlichen r von einander verschiedenen ursprünglichen Classen erster Art, welche mit S componirt die Classe S selbst hervorbringen; da aus $SR = S$ und $SR' = S$ auch $S(RR') = S$ folgt, so bilden diese r Classen eine Gruppe $\mathfrak{R}$ vom Grade r; und da das System aller h ursprünglichen Classen erster Art ebenfalls eine Gruppe $\mathfrak{H}$ bildet, welche ein Multiplum der Gruppe $\mathfrak{R}$ ist (§. 149), so ist $h = rk$, und die Gruppe $\mathfrak{H}$ zerfällt in k Complexe von der Form $\mathfrak{R}H$; alle r Classen eines solchen Complexes $\mathfrak{R}H$ geben, mit S componirt, eine und dieselbe Classe SH vom Theiler σ; und umgekehrt, wenn $SH' = SH$ ist, so folgt $SH'H^{-1} = S$, also ist $H'H^{-1} = R$ in $\mathfrak{R}$, mithin $H' = RH$ in dem Complex $\mathfrak{R}H$ enthalten. Die Anzahl h' der verschiedenen Classen vom Theiler σ ist daher $= k$, und wir sind also zu folgendem Resultate gelangt:

Die Anzahl h der ursprünglichen Classen der ersten Art ist $r$mal so gross als die Anzahl h' der Classen vom Theiler σ, wo r die Anzahl derjenigen ursprünglichen Classen der ersten Art bedeutet, welche mit der einfachsten Classe vom Theiler σ zusammengesetzt diese letztere wieder erzeugen.

Dies Resultat behält offenbar seine Gültigkeit für eine negative Determinante, auch wenn nicht alle, sondern nur die sogenannten positiven Classen gezählt werden (§. 64).

Es kommt jetzt offenbar nur noch darauf an, die Anzahl r zu bestimmen, und zu diesem Zwecke stellt *Gauss* folgenden schönen Satz auf:

Die r ursprünglichen Classen der ersten Art, welche mit der einfachsten Classe vom Theiler σ zusammengesetzt diese letztere wieder erzeugen, sind identisch mit denjenigen Classen, durch deren Formen das Quadrat des Theilers σ eigentlich oder uneigentlich dargestellt werden kann.

Um denselben zu beweisen, bemerken wir zunächst, dass man als Repräsentanten einer *jeden* ursprünglichen Classe H der ersten Art stets eine Form $(a, B, C\sigma)$ annehmen kann, in welcher a relative Primzahl zu σ ist, $2B$ und C aber durch σ theilbar sind; hat man nämlich (nach §. 93) als Repräsentanten zunächst eine Form (a, b, c) gewählt, in welcher a relative Primzahl zu σ ist, und componirt man dieselbe mit einer Form (σ, b', c') aus der einfachsten Classe S vom Theiler σ, so erhält man (§§. 146, 147) eine Form

$(a\sigma, B, C)$ vom Theiler σ, und zwar so, dass die Formen (a, b, c), (σ, b', c') resp. den Formen $(a, B, C\sigma)$, (σ, B, aC) äquivalent sind; es kann daher $(a, B, C\sigma)$ statt (a, b, c) als Repräsentant der Classe H gewählt werden.

Ist nun $SH = S$, also H eine der r Classen aus der Gruppe $\mathfrak{R}$, so ist $(a\sigma, B, C)$ äquivalent mit (σ, B, aC), und folglich existiren zwei ganze Zahlen x, y, welche der Bedingung

$$a\sigma x^2 + 2Bxy + Cy^2 = \sigma$$

genügen; hieraus folgt aber

$$a(\sigma x)^2 + 2B(\sigma x)y + C\sigma y^2 = \sigma^2,$$

d. h. σ^2 wird durch die Form $(a, B, C\sigma)$ der Classe H dargestellt, wenn den Variabeln die Werthe σx, y beigelegt werden.

Umgekehrt, ist σ^2 durch die Formen der Classe H, also auch durch die Form $(a, B, C\sigma)$ darstellbar, so existiren zwei ganze Zahlen x', y, welche der Bedingung

$$ax'^2 + 2Bx'y + C\sigma y^2 = \sigma^2$$

genügen. Zunächst ergiebt sich hieraus, dass x' durch σ theilbar sein muss; denn da C und $2B$, also auch $2By = \beta\sigma$ durch σ theilbar ist, so folgt $ax'^2 + \beta\sigma x' \equiv 0 \pmod{\sigma^2}$; ist nun δ der grösste gemeinschaftliche Divisor von $x' = \delta x$ und $\sigma = \delta\varrho$, wo also x und ϱ relative Primzahlen bedeuten, so ergiebt sich $ax^2 + \beta\varrho x \equiv 0 \pmod{\varrho^2}$, also muss ax^2, folglich auch a durch ϱ theilbar sein; da aber a relative Primzahl zu $\sigma = \delta\varrho$, also auch zu ϱ ist, so muss $\varrho = 1$, $\delta = \sigma$, also $x' = \sigma x$ sein. Nachdem dies bewiesen ist, ergiebt sich

$$a\sigma x^2 + 2Bxy + Cy^2 = \sigma;$$

da ferner $2B$ und C durch σ theilbar sind, so folgt, dass x und y relative Primzahlen sind; mithin ist σ eigentlich darstellbar durch die Form $(a\sigma, B, C)$ vom Theiler σ, welche folglich (§. 60) einer Form äquivalent sein muss, deren erster Coefficient $= \sigma$ ist, und die also der einfachsten Classe S vom Theiler σ angehört. Da nun $(a\sigma, B, C)$ auch der Classe SH angehört, so ist $SH = S$, d. h. H ist eine Classe aus der Gruppe $\mathfrak{R}$, was zu beweisen war.

Durch den hiermit bewiesenen obigen Satz sind wir nun in den Stand gesetzt, den Grad r der Gruppe $\mathfrak{R}$ genau zu bestimmen. Ist R eine Classe aus dieser Gruppe, und wird σ^2 durch ihre Formen so dargestellt, dass die beiden darstellenden Zahlen (x, y) den grössten gemeinschaftlichen Theiler δ haben, so geht δ^2 in σ^2, folg-

lich δ in $\sigma = \delta\varrho$ auf; mithin ist (nach §. 60) ϱ^2 eigentlich darstellbar durch die Formen der Classe R, und folglich kann man (nach §. 60) als Repräsentanten von R eine Form wählen, deren erster Coefficient $= \varrho^2$ ist. Da umgekehrt durch jede solche Form auch σ^2 dargestellt wird, wenn den Variabelen die Werthe $x = \delta$, $y = 0$ ertheilt werden, so gehört sie, wenn sie zugleich ursprünglich von der ersten Art ist, einer Classe R aus der Gruppe $\mathfrak{R}$ an. Wir haben mithin folgenden Satz erhalten:

Der Grad r der Gruppe $\mathfrak{R}$ ist gleich der Anzahl aller nicht äquivalenten ursprünglichen Formen der ersten Art, deren erster Coefficient ein quadratischer Divisor ϱ^2 vom Quadrate des Theilers σ ist.

Wir bemerken schliesslich, dass für jeden solchen quadratischen Divisor ϱ^2 (zufolge §. 56) nur alle diejenigen Formen zu untersuchen sind, deren mittlere Coefficienten ein vollständiges Restsystem nach dem Modulus ϱ^2 bilden.

§. 151.

Nachdem im Vorhergehenden der Weg allgemein vorgezeichnet ist, auf welchem man zur Bestimmung des Verhältnisses der Classenanzahlen h und h' gelangt, schreiten wir zur Betrachtung der speciellen Fälle, in welchen σ eine *Primzahl* ist, weil aus ihnen das allgemeine Resultat abgeleitet werden kann.

I. Ist die Determinante $D = 1 - 4n \equiv 1 \pmod 4$, und $\sigma = 2$, so handelt es sich um die Vergleichung der Classenanzahlen der ursprünglichen Formen der ersten und zweiten Art. Bezeichnet man dieselben wieder mit h und h', so ist $h = rh'$, wo r die Anzahl der nicht äquivalenten ursprünglichen Formen erster Art bedeutet, deren erster Coefficient $= 1$ oder $= 4$ ist. Da im zweiten Fall der mittlere Coefficient ungerade sein muss, so sind nur die drei Formen

$$(1, 0, -D), (4, \pm 1, n)$$

in Betracht zu ziehen.

Ist $D \equiv 1 \pmod 8$, also n gerade, so ist nur die erste dieser Formen ursprünglich von der ersten Art, folglich $r = 1$, und $h = h'$.

Ist aber $D \equiv 5 \pmod 8$, also n ungerade, so sind alle drei Formen ursprünglich von der ersten Art, und es braucht nur noch untersucht zu werden, ob sie verschiedenen Classen angehören oder nicht. Zunächst lässt sich beweisen, dass sie entweder zu einer und derselben, oder zu drei verschiedenen Classen gehören. *Gauss* zeigt dies durch die Composition der ihnen entsprechenden Classen $1, P, Q$; da die Classen P, Q entgegengesetzt sind, so ist $PQ = 1$, und ferner lässt sich leicht zeigen, dass $PP = Q$ und $QQ = P$ ist (denn aus den beiden einigen, in P enthaltenen Formen $(4, 1, n)$, $(n, -1, 4)$ ist die Form $(4n, 2n-1, n)$ zusammengesetzt, und da diese mit $(n, 1-2n, 4n)$, $(n, 1, 4)$, $(4, -1, n)$ äquivalent ist, so folgt $PP = Q$); nimmt man nun an, dass zwei der drei Classen 1, P, Q identisch sind, so ergiebt sich hieraus sofort, dass auch die dritte mit ihnen übereinstimmt. Dasselbe lässt sich auch durch die folgenden Sätze erweisen.

Sind irgend zwei der drei Formen $(1, 0, -D)$, $(4, \pm 1, n)$ *äquivalent, so ist die Gleichung* $t^2 - Du^2 = 4$ *durch ungerade Zahlen* t, u *lösbar.*

Ist nämlich die erste Form mit einer der beiden anderen äquivalent, so ist (nach §. 60) der erste Coefficient 4 dieser letztern eigentlich darstellbar durch die Form $(1, 0, -D)$, also giebt es zwei relative Primzahlen t, u, welche der Gleichung $t^2 - Du^2 = 4$ genügen, woraus folgt, dass t, u, da sie nicht beide gerade sein können, nothwendig beide ungerade sein müssen. Sind ferner die beiden letzten Formen äquivalent, so giebt es (nach §. 60. Anm.) zwei ganze Zahlen x, y, welche den Bedingungen

$$4x^2 + 2xy + ny^2 = 4, \quad -2x + ny \equiv 0 \pmod 4$$

genügen; da n ungerade ist, so muss y gerade sein $= 2u$; setzt man dann $2x + u = t$, so gehen diese Bedingungen in die folgenden über

$$t^2 - Du^2 = 4, \; t \equiv -u \pmod 4;$$

da aus der letztern $t^2 \equiv u^2 \pmod 8$ folgt, und ausserdem $-D \equiv 3 \pmod 8$ ist, so folgt aus der erstern $4u^2 \equiv 4 \pmod 8$, mithin ist u, also auch t ungerade, was zu beweisen war.

Ist die Gleichung $t^2 - Du^2 = 4$ *durch ungerade Zahlen* t, u *lösbar, so sind alle drei Formen* $(1, 0, -D)$, $(4, \pm 1, n)$ *äquivalent.*

Denn wenn man t mit beliebigem Vorzeichen, dann aber $u \equiv -t \pmod 4$ wählt, so geht die Form $(1, 0, -D)$ durch die Substitutionen

$$\begin{pmatrix} t, & \pm\dfrac{t+Du}{4} \\ \pm u, & \dfrac{t+u}{4} \end{pmatrix}$$

in die beiden Formen $(4, \pm 1, n)$ über. — Durch Verbindung der beiden vorstehenden Sätze ergiebt sich:

Die drei obigen Formen sind äquivalent oder gehören drei verschiedenen Classen an, je nachdem die Gleichung $t^2 - Du^2 = 4$ durch ungerade Zahlen t, u lösbar ist oder nicht; im ersten Falle ist $h = h'$, im zweiten $h = 3h'$.

Ist nun D positiv, so tritt der erste Fall ein oder der zweite, je nachdem die *kleinste* Lösung $t = T'$, $u = U'$ aus ungeraden oder geraden Zahlen besteht. Ist D negativ, so besitzt die Gleichung im Allgemeinen nur die beiden Auflösungen $t = \pm 2$, $u = 0$, und mithin ist $h = 3h'$; die einzige Ausnahme hiervon bildet die Determinante $D = -3$, weil die Gleichung ausser den beiden Lösungen $t^2 = 4$, $u = 0$ noch die vier Lösungen $t^2 = u^2 = 1$ besitzt, und folglich ist in diesem Falle wieder $h = h'$.

Diese Resultate stimmen vollkommen mit denjenigen überein, welche wir früher (§§. 97, 99) mit Hülfe ganz anderer Principien abgeleitet haben.

II. Ist $D = D'\sigma^2$, so leuchtet ein, dass h' zugleich die Anzahl der ursprünglichen Classen erster Art von der Determinante D' ist. Unter der Voraussetzung, dass σ eine Primzahl ist, haben wir, um das Verhältniss $r = h : h'$ zu bestimmen, nur die l Formen

$$(1, 0, -D) \text{ und } (\sigma^2, B\sigma, BB - D') \qquad (1)$$

zu betrachten, wo B ein vollständiges Restsystem (mod. σ) durchlaufen muss, mit Ausnahme derjenigen Werthe, für welche $BB \equiv D'$ (mod. σ) wird, weil diesen keine ursprünglichen Formen entsprechen; die Anzahl der zu betrachtenden ursprünglichen Formen ist daher

$$l = 2 \text{ oder } \sigma - \left(\frac{D'}{\sigma}\right) \qquad (2)$$

je nachdem $\sigma = 2$ oder eine ungerade Primzahl ist. Zur Bestimmung der Anzahl r der verschiedenen Classen, welchen diese l Formen angehören, gelangen wir durch die folgenden Sätze.

Die beiden Formen $(1, 0, -D)$, $(\sigma^2, \beta\sigma, \beta\beta - D')$ *sind stets und nur dann äquivalent, wenn es zwei ganze Zahlen* t', u' *giebt, welche den Bedingungen*

$$t't' - D'u'u' = 1, \quad t' + \beta u' \equiv 0 \ (mod.\ \sigma) \tag{3}$$

genügen; zwei Formen $(\sigma^2, b\sigma, bb - D')$, $(\sigma^2, b'\sigma, b'b' - D')$ *sind stets und nur dann äquivalent, wenn es zwei ganze Zahlen* t', u' *giebt, welche den Bedingungen*

$$t't' - D'u'u' = 1, \ (b - b')t' + (bb' - D')u' \equiv 0 \ (mod.\ \sigma) \tag{4}$$

genügen.

Die Aequivalenz der Formen $(1, 0, -D)$, $(\sigma^2, \beta\sigma, \beta\beta - D')$ ist (nach §. 60 Anmerkung) gleichbedeutend mit der Annahme der Existenz zweier ganzen Zahlen x, y, welche die Bedingungen

$$x^2 - D'\sigma^2y^2 = \sigma^2,$$
$$x + \beta\sigma y \equiv 0, \ -\beta\sigma x - D'\sigma^2 y \equiv 0 \ (\text{mod. } \sigma^2)$$

erfüllen; da nun aus der ersten folgt, dass x durch σ theilbar ist, und da sie durch die Substitutionen $x = \sigma t', y = u'$ in die Bedingungen (3) übergehen, aus welchen sie umgekehrt folgen, so ist der erste Theil des Satzes erwiesen. Ebenso fällt die Annahme der Aequivalenz der Formen $(\sigma^2, b\sigma, bb - D')$, $(\sigma^2, b'\sigma, b'b' - D')$ zusammen mit der Annahme der Existenz zweier ganzen Zahlen x, y, welche die Bedingungen

$$\sigma^2x^2 + 2b\sigma xy + (bb - D')y^2 = \sigma^2,$$
$$\sigma^2x + (b + b')\sigma y \equiv 0, \ (b - b')\sigma x + (bb - D')y \equiv 0 \ (\text{mod. } \sigma^2)$$

befriedigen; da nun der Voraussetzung nach $bb - D'$ nicht durch σ theilbar ist, so muss y^2 und folglich auch y durch die Primzahl σ theilbar sein; da ferner die vorstehenden Bedingungen durch die Substitution $y = \sigma u', x = t' - bu'$ in die Bedingungen (4) übergehen, aus denen sie auch rückwärts folgen, so ist auch der zweite Theil des obigen Satzes bewiesen.

Bedeutet λ *die Anzahl derjenigen Formen* (1), *welche der Hauptclasse angehören, so ist* $l = r\lambda$.

Gehört die Form $(\sigma^2, \beta\sigma, \beta^2 - D')$ der Hauptclasse an, so existirt eine Lösung (t', u') der Gleichung

$$t't' - D'u'u' = 1 \tag{5}$$

welche der Congruenz $t' + \beta u' \equiv 0$ (mod. σ) genügt, und folglich kann u' nicht durch σ theilbar sein. Ist umgekehrt (t', u') eine Lösung der Gleichung (5), und u' nicht theilbar durch σ, so existirt

stets eine und nur eine Zahlclasse β (mod. σ), welche der Congruenz $t' + \beta u' \equiv 0$ (mod. σ) genügt, und ihr entspricht eine zur Hauptclasse gehörige Form $(\sigma^2, \beta\sigma, \beta^2 - D')$. Um also alle diese Formen zu erhalten, muss man alle Lösungen (t', u') der Gleichung (5) aufstellen, in welchen u' nicht durch σ theilbar ist, und jedesmal die entsprechende Zahlclasse β (mod. σ) durch die Congruenz $t' + \beta u' \equiv 0$ (mod. σ) bestimmen. Da ausserdem die Form $(1, 0, -D)$ zur Hauptclasse gehört, und λ die Anzahl aller zur Hauptclasse gehörenden Formen (1) bedeutet, so ist also $\lambda - 1$ die Anzahl der sämmtlichen incongruenten Zahlclassen β (mod. σ), welche aus Lösungen (t', u') der Gleichung (5) vermöge der Congruenz $t' + \beta u' \equiv 0$ (mod. σ) erzeugt werden können.

Sind hierdurch schon alle Formen (1) erschöpft, so ist $l = \lambda$ und $r = 1$, also der Satz richtig. Giebt es aber eine nicht zur Hauptclasse gehörende ursprüngliche Form $(\sigma^2, b'\sigma, b'b' - D')$, d.h. giebt es eine von den $\lambda - 1$ Zahlclassen β (mod. σ) verschiedene Zahlclasse b' von der Beschaffenheit, dass $b'b' - D'$ nicht durch σ theilbar ist, so wollen wir zeigen, dass unter den l Formen (1) sich genau $(\lambda - 1)$ Formen $(\sigma^2, b\sigma, bb - D')$ finden, welche alle mit der Form $(\sigma^2, b'\sigma, b'b' - D')$ äquivalent und von ihr verschieden sind. Ist nämlich $(\sigma^2, b\sigma, bb - D')$ eine solche Form, also $b - b'$ nicht durch σ theilbar, so giebt es, wie oben gezeigt ist, eine Lösung (t', u') der Gleichung (5), welche der Congruenz

$$(b - b')t' + (bb' - D')u' \equiv 0 \text{ (mod. } \sigma) \qquad (4)$$

genügt, aus welcher zugleich folgt, dass u' nicht durch σ theilbar ist. Umgekehrt, ist (t', u') eine Lösung der Gleichung (5), in welcher u' nicht durch σ theilbar ist, und $t' + \beta u' \equiv 0$ (mod. σ), so existirt, weil $b' - \beta$ nicht durch σ theilbar ist, immer eine und nur eine Zahlclasse b (mod. σ), welche die Congruenz

$$(b' - \beta)\, b \equiv D' - b'\beta \text{ (mod. } \sigma) \qquad (6)$$

befriedigt, und zwar kann b nicht $\equiv b'$ (mod. σ) sein, weil hieraus $b'b' \equiv D'$ (mod. σ) folgen würde; multiplicirt man nun (6) mit u', so ergiebt sich (4), und folglich ist wirklich $(\sigma^2, b\sigma, bb - D')$ äquivalent mit der Form $(\sigma^2, b'\sigma, b'b' - D')$ und zugleich verschieden von ihr, weil $b - b'$ nicht durch σ theilbar ist. Um also alle mit der Form $(\sigma^2, b'\sigma, b'b' - D')$ äquivalenten und von ihr verschiedenen Formen $(\sigma^2, b\sigma, bb - D')$ zu erhalten, braucht man nur die sämmtlichen $(\lambda - 1)$ Congruenzen (6) aufzustellen, welche den $(\lambda - 1)$ incongruenten Zahlclassen β (mod. σ) entsprechen, und für

jede die entsprechende Zahlclasse b zu bestimmen. Auf diese Weise entstehen aber wirklich auch $(\lambda - 1)$ verschiedene Zahlclassen $b \pmod{\sigma}$; denn wollte man annehmen, es könnte zwei verschiedenen Zahlclassen β, $\beta' \pmod{\sigma}$ eine und dieselbe Zahlclasse $b \pmod{\sigma}$ entsprechen, so wäre

$$(b'-\beta)b \equiv D'-b'\beta,\ (b'-\beta')b \equiv D'-b'\beta' \pmod{\sigma};$$

hieraus würde aber durch Subtraction $(\beta'-\beta)(b-b') \equiv 0 \pmod{\sigma}$ folgen, was unmöglich ist, da weder $\beta'-\beta$ noch $b-b'$ durch σ theilbar ist. Mithin giebt es wirklich genau $\lambda - 1$ verschiedene Formen $(\sigma^2, b\sigma, bb-D')$, welche mit der Form $(\sigma^2, b'\sigma, b'b'-D')$ äquivalent und zugleich von ihr verschieden sind. Von den l Formen (1) gehören daher immer je λ, und nicht mehr, zu einer und derselben Classe, folglich ist $l = r\lambda$, was zu beweisen war.

Ist die Determinante $D = D'\sigma^2$ negativ, so ist h im Allgemeinen $= lh'$, und nur dann $= \frac{1}{2}lh'$, wenn $D' = -1$.

Denn die Gleichung (5) besitzt nur im letztern Falle Lösungen $(t' = 0, u' = \pm 1)$, in welchen u' nicht durch σ theilbar ist; da denselben nur die eine Zahlclasse $\beta \equiv 0 \pmod{\sigma}$ entspricht, so ist $\lambda = 2$, also $r = \frac{1}{2}l$; in allen anderen Fällen ist $\lambda = 1$, also $r = l$.

Ist die Determinante $D = D'\sigma^2$ positiv, so ist $h \log(T + U\sqrt{D}) = l.h' \log(T' + U'\sqrt{D'})$, wo (T, U), (T', U') resp. die kleinsten positiven Auflösungen der Gleichungen $T^2 - DU^2 = 1$, $T'^2 - D'U'^2 = 1$ bedeuten.

Um dies zu beweisen, schicken wir eine Bemerkung über die Lösungen der Gleichung (5) voraus. Wenn zwei solche Lösungen (t', u'), (t'', u'') der Bedingung

$$t'u'' - u't'' \equiv 0 \pmod{\sigma} \tag{7}$$

genügen, so kann man, wenn $\sqrt{D'}$ und $\sqrt{D} = \sigma\sqrt{D'}$ immer positiv genommen werden,

$$t' + u'\sqrt{D'} = (t'' + u''\sqrt{D'})\,(t + u\sqrt{D}), \tag{8}$$

setzen, wo die ganzen Zahlen t, u eine Lösung der Gleichung

$$t^2 - Du^2 = 1 \tag{9}$$

bilden. Umgekehrt, sind (t'', u''), (t, u) resp. Lösungen der Gleichungen (5), (9), so liefert die Gleichung (8) stets eine Lösung (t', u') der Gleichung (5), welche zugleich der Bedingung (7) genügt. Je zwei solche Lösungen (t', u'), (t'', u'') der Gleichung (5) wollen wir äquivalent nennen; dann leuchtet sofort ein, dass zwei Lö-

sungen, welche einer dritten äquivalent sind, auch einander äquivalent sein müssen. Man kann daher die sämmtlichen Lösungen der Gleichung (5) in Classen eintheilen, deren jede alle und nur solche Lösungen enthält, die unter einander äquivalent sind. Da nun die Gleichung (8) lehrt, aus einer gegebenen Lösung (t'', u'') alle ihr äquivalenten Lösungen (t', u') zu finden, und da $t + uV D = \pm (T + UV D)^n$ ist, wo das Vorzeichen nach Belieben, und für n jede ganze Zahl gewählt werden darf (§. 85), so leuchtet ein (vergl. §. 87), dass aus jeder Classe von Lösungen ein und nur ein Repräsentant (t', u') so gewählt werden kann, dass

$$1 \leqq t' + u' V D' < T + UV D$$

wird; da ferner $(T, U\sigma)$ ebenfalls eine Lösung der Gleichung (5), und folglich (§. 85)

$$T + UV D = (T' + U' V D')^{\lambda'}$$

ist, wo λ' eine bestimmte positive ganze Zahl bedeutet, so leuchtet ein, dass die ersten Factoren $t' + u' V D'$ der obigen Repräsentanten (t', u') von der Form $(T' + U' V D')^{n'}$ sind, wo n' die λ' Werthe $0, 1, 2 \ldots (\lambda' - 1)$ durchlaufen muss, dass also die Anzahl der Classen $= \lambda'$ ist.

Die erste von diesen Classen enthält also die Lösungen (t', u') und nur solche, deren zweite Elemente u' durch σ theilbar sind. Jede Lösung (t', u') aus einer der übrigen $\lambda' - 1$ Classen liefert aber durch die Congruenz $t' + \beta u' \equiv 0 \pmod{\sigma}$ eine zugehörige Zahlclasse $\beta \pmod{\sigma}$, und da unmittelbar einleuchtet, dass zwei solche Lösungen stets und nur dann zu derselben Zahlclasse $\beta \pmod{\sigma}$ führen, wenn sie derselben Classe von Lösungen angehören, so muss die Anzahl $\lambda - 1$ der Zahlclassen β mit der Anzahl $\lambda' - 1$ dieser Classen von Lösungen übereinstimmen; also ist $\lambda = \lambda'$, was zu beweisen war.

Offenbar lässt sich aus dem hier behandelten speciellen Fall ohne Schwierigkeit das in §. 100 erhaltene Resultat für den allgemeinen Fall ableiten, in welchem σ eine beliebige zusammengesetzte Zahl ist.

§. 152.

Wir beschränken uns nun im Folgenden auf die Composition von ursprünglichen Classen erster Art, und behalten ausserdem, wenn die Determinante D negativ ist, nur die positiven Classen bei, deren Zusammensetzung offenbar immer wieder zu positiven Classen führt. Diese h Classen, welche eine Gruppe $\mathfrak{H}$ bilden, zerfallen (§. 122) je nach dem Ausfall der λ Charaktere C, welche dieser Determinante D entsprechen, in Geschlechter, und es ist mit Hülfe des Reciprocitätssatzes gezeigt (§. 123), dass *höchstens* der Hälfte aller angebbaren Totalcharaktere wirklich existirende Classen entsprechen. *Gauss**) leitet nun diesen letzteren Satz aus der Theorie der Composition ab, und er benutzt ihn, um darauf einen neuen, den *zweiten* Beweis des Reciprocitätssatzes zu gründen. Da diese tiefsinnigen Principien sich auf die Beweise von höheren Reciprocitätsgesetzen übertragen lassen**), so theilen wir dieselben in diesem und den folgenden Paragraphen mit.

Sind ε, ε' die Werthe eines Charakters C resp. für die Classen H, H', so ist $C = \varepsilon\varepsilon'$ für die Classe HH'.

Man kann als Repräsentanten der Classen H, H' immer zwei einige Formen nehmen, deren erste Coefficienten a, a' relative Primzahlen zu $2D$ sind; da die aus ihnen zusammengesetzte, also der Classe HH' angehörende Form den ersten Coefficienten aa' hat, welcher ebenfalls relative Primzahl zu $2D$ ist, so ergiebt sich der zu beweisende Satz unmittelbar, wenn man bedenkt, dass der Charakter C oder $C(n)$ ein Ausdruck von der Art

$$(-1)^{\frac{1}{2}(n-1)},\ (-1)^{\frac{1}{8}(n^2-1)},\ (-1)^{\frac{1}{2}(n-1)+\frac{1}{8}(n^2-1)},\ \left(\frac{n}{l}\right)\cdots$$

ist (§. 122), und dass folglich die drei Werthe $C(a)$, $C(a')$, $C(aa')$, welche dieser Charakter resp. in den drei Classen H, H', HH' besitzt, der Bedingung $C(a)\,C(a') = C(aa')$ genügen.

Aus diesem Satze ergiebt sich, dass, wenn die Classen K, K' resp. denselben Geschlechtern G, G' angehören, wie die Classen

---

*) *D. A.* artt. 257—262.

**) *Kummer: Ueber die allgemeinen Reciprocitätsgesetze unter den Resten und Nichtresten der Potenzen, deren Grad eine Primzahl ist.* 1859. Vergl. Berliner Monatsbericht vom 18. Febr. 1858.

H, H', dann auch die Classen KK' und HH' sich in einem und demselben Geschlechte finden, welches das *aus G, G' zusammengesetzte Geschlecht* heissen soll*). Sind ferner N, N' zwei Classen des *Hauptgeschlechtes*, d. h. desjenigen Geschlechtes, in welchem sich die Hauptform $(1, 0, -D)$ findet, und folglich alle Charaktere C den Werth $+1$ haben, so gehört die zusammengesetzte Classe NN' ebenfalls diesem Geschlechte an, mithin bilden alle n Classen des Hauptgeschlechtes eine Gruppe $\mathfrak{N}$ vom Grade n (§. 149); zugleich zerfallen die sämmtlichen h Classen in g Complexe $\mathfrak{N}H$ von je n Classen, welche jedesmal einem und demselben Geschlecht angehören; zwei verschiedene solche Complexe gehören, wie man leicht erkennt, auch zu verschiedenen Geschlechtern; mithin ist $h = ng$, und g die Anzahl der wirklich existirenden von einander verschiedenen Geschlechter**).

Die Determinante D heisst *regulär* oder *irregulär*, je nachdem die von den n Classen des Hauptgeschlechtes gebildete Gruppe regulär ist oder nicht (§. 149); bedeutet im letztern Falle δ den Grad der grössten in ihr enthaltenen regulären Gruppe, so heisst die ganze Zahl $n:\delta$ der *Irregularitätsexponent* der Determinante***).

Aus dem obigen Satze über den Charakter einer zusammengesetzten Classe ergiebt sich ferner unmittelbar der folgende:

Jede Classe Q, welche durch Duplication einer Classe entsteht, gehört dem Hauptgeschlechte an.

Die Anzahl q der verschiedenen Classen Q, welche durch Duplication der sämmtlichen h Classen entstehen, ist daher $\leqq n$ (da diese Classen, wie leicht zu ersehen ist, eine Gruppe Ω bilden, so muss q gewiss ein Divisor von n sein). Um sie genauer zu bestimmen, nehmen wir an, Q entstehe durch Duplication der bestimmten Classe H, und fragen nach allen Classen H', durch deren Duplication dieselbe Classe Q entsteht. Aus der Annahme $H'H' = Q = HH$ folgt nun, wenn man $H' = AH$ setzt, $AA = 1$, also $A = A^{-1}$, d. h. die Classe A ist identisch mit der ihr entgegengesetzten Classe, und folglich ist sie eine *ambige* Classe (§. 148, 2., §§. 56 — 58). Umgekehrt, ist $H' = AH$, und A eine ambige Classe, so ist auch $H'H' = HH$. Schreibt man daher alle α ambigen Classen A auf, welche offenbar eine Gruppe $\mathfrak{A}$ bilden, so zerfallen alle h Classen

*) *Gauss: D. A.* artt. 246, 247.
**) *Gauss: D. A.* art. 252.
***) *Gauss: D. A.* art. 306. VII.

in q Complexe $\mathfrak{A}H$ von je α Classen, deren Duplication eine und dieselbe Classe HH hervorbringt, während zwei Classen, welche zwei verschiedenen solchen Complexen angehören, durch Duplication auch zwei verschiedene Classen hervorbringen; und endlich ist $h = \alpha q$.

Da nun h auch $= ng$, und ausserdem $q \leqq n$ ist, so ergiebt sich $g \leqq \alpha$, d. h. der Satz: *Die Anzahl der wirklich existirenden verschiedenen Geschlechter ist höchstens gleich der Anzahl der ambigen Classen.*

§. 153.

Es kommt also jetzt darauf an, für eine gegebene Determinante D die Anzahl α aller ambigen Classen A genau zu bestimmen, welche ursprünglich von erster Art sind.

Da in jeder ambigen Classe $A = A^{-1}$ stets mindestens eine ambige Form (a, b, c) zu finden ist (§. 58), so bleibt gewiss keine jener α Classen unvertreten, wenn wir alle ambigen Formen aufschreiben. Da nun in einer solchen Form $2b$ durch a theilbar, folglich b entweder $\equiv 0$, oder $\equiv \frac{1}{2}a \pmod{a}$, also (a, b, c) selbst mit einer Form äquivalent ist (§. 56), deren mittlerer Coefficient entweder Null, oder die Hälfte des ersten Coefficienten ist, so genügt es, alle Formen

$$\left(a, 0, \frac{-D}{a}\right) \quad \text{und} \quad \left(2b, b, \frac{b^2 - D}{2b}\right)$$

zu betrachten, welche ursprünglich von erster Art sind.

Bedeutet μ die Anzahl aller verschiedenen *ungeraden* Primzahlen, welche in D aufgehen, ist ferner $\nu = 0$ oder $= 1$, je nachdem D ungerade oder gerade, so ist $\mu + \nu$ die Anzahl *aller* verschiedenen in D aufgehenden Primzahlen. Dann leuchtet ein, dass die Anzahl aller ursprünglichen Formen vom Typus

$$(a, 0, a')$$

gleich $2^{\mu+\nu+1}$ ist; die eine Hälfte derselben hat positive erste Coefficienten, die andere Hälfte negative.

Betrachten wir nun die anderen ambigen ursprünglichen Formen erster Art, deren Typus

$$\left(2b,\ b,\ \frac{b^2-D}{2b}\right)$$

ist, so muss b ein solcher Divisor von $D = -bb'$ sein, dass der dritte Coefficient $\frac{1}{2}(b+b')$ eine ganze Zahl und relative Primzahl zu $2b$ wird; mithin muss zunächst $b+b' \equiv 2 \pmod 4$ sein, und ferner dürfen b und b' keinen gemeinschaftlichen ungeraden Divisor haben. Sind nun b und b' ungerade, so folgt $b' \equiv b$, $D \equiv -bb \equiv 3 \pmod 4$; umgekehrt, wenn $D \equiv 3 \pmod 4$, so kann b nur ungerade sein, und aus $bb' = -D \equiv 1 \pmod 4$ folgt von selbst, dass $b \equiv b'$, also $b+b' \equiv 2 \pmod 4$ wird; mithin kann b jeder Divisor von D sein, für welchen b und b' relative Primzahlen werden. Die Anzahl dieser Formen

$$(2b,\ b,\ \tfrac{1}{2}(b+b'))$$

ist daher $= 2^{\mu+1}$, unter welchen ebensoviele mit positiven, wie mit negativen ersten Coefficienten vorkommen. Sind aber b und b' gerade, so ist eine von ihnen $\equiv 0$, die andere $\equiv 2 \pmod 4$, mithin $D \equiv 0 \pmod 8$, und $\frac{1}{2}b$, $\frac{1}{2}b'$ sind relative Primzahlen. Umgekehrt, wenn $D \equiv 0 \pmod 8$ ist, so muss b gerade sein, und man kann für $\frac{1}{2}b$ jeden Divisor von $\frac{1}{4}D = -\frac{1}{2}b \cdot \frac{1}{2}b'$ wählen, für welchen $\frac{1}{2}b$, $\frac{1}{2}b'$ relative Primzahlen werden; mithin ist die Anzahl dieser Formen, da $\frac{1}{4}D$ gerade ist, gleich $2^{\mu+2}$, und unter ihnen finden sich ebensoviele mit positiven wie mit negativen ersten Coefficienten.

Die Anzahl aller dieser ambigen ursprünglichen Formen erster Art ist daher gleich

$$\begin{aligned} &2^{\mu+1}, \text{ wenn } && D \equiv 1 \pmod 4, \\ &2^{\mu+2}, && D \equiv 2, 3, 4, 6, 7 \pmod 8, \\ &2^{\mu+3}, && D \equiv 0 \pmod 8; \end{aligned}$$

sie ist folglich in allen Fällen genau doppelt so gross, als die Anzahl $2^\lambda = 2\tau$ aller angebbaren Totalcharaktere für die Determinante D (§. 122). Es kommt jetzt darauf an, die Anzahl der verschiedenen Classen zu bestimmen, welche durch diese Formen repräsentirt werden.

Sieht man von dem singulären Fall $D = -1$ vorläufig ganz ab, so erkennt man leicht, dass die Coefficienten a und a', ebenso die Zahlen b und b', selbst ihren absoluten Werthen nach, von einander verschieden sein müssen. Hätten nämlich die relativen Primzahlen a, a' denselben absoluten Werth 1, so wäre $D = \pm 1$; dasselbe würde sich ergeben, wenn man annehmen wollte, die unge-

raden Zahlen b und b' hätten denselben absoluten Werth; sind endlich b und b' gerade, so ist die eine der Zahlen $\frac{1}{2}b$, $\frac{1}{2}b'$ gerade, die andere ungerade, also haben sie verschiedene absolute Werthe. Hieraus folgt, dass die sämmtlichen obigen Formen immer in Paare von je zwei von einander verschiedenen Formen $(a, 0, a')$, $(a', 0, a)$, und $(2b, b, \frac{1}{2}(b+b'))$, $(2b', b', \frac{1}{2}(b+b'))$ zerfallen, und da die erste resp. durch die Substitutionen $\left(\begin{smallmatrix}0, & 1\\ -1, & 0\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}-1, & -1\\ +2, & +1\end{smallmatrix}\right)$ in die zweite übergeht, so genügt es, diejenige von ihnen beizubehalten, deren erster Coefficient der kleinere ist; mithin haben wir nur noch 2τ Formen $(a, 0, a')$, $(2b, b, \frac{1}{2}(b+b'))$, in welchen die absoluten Werthe (a) und $(b) < \sqrt{(D)}$ sind; und unter diesen Formen giebt es wieder ebensoviele mit positiven ersten Coefficienten, wie mit negativen.

Ist nun D *negativ*, so behalten wir nur die τ Formen bei, deren äussere Coefficienten positiv sind, und wir wollen zeigen, dass sie die Repräsentanten von ebensovielen verschiedenen Classen sind. Zunächst sind alle Formen $(a, 0, a')$ und diejenigen Formen $(2b, b, \frac{1}{2}(b+b'))$, in welchen $3b \leqq b'$ ist, *reducirt* (§. 64), und statt jeder nicht reducirten Form $(2b, b, \frac{1}{2}(b+b'))$, in welcher also $3b > b'$, können wir die ihr nach rechts benachbarte reducirte Form $(\frac{1}{2}(b+b'), \frac{1}{2}(b'-b), \frac{1}{2}(b+b'))$ substituiren. Man erkennt nun leicht, dass alle diese τ reducirten Formen von einander verschieden, und dass auch keine zwei einander entgegengesetzt sind, weil keiner der mittleren Coefficienten negativ ist; sie gehören daher (§. 65) ebensovielen verschiedenen Classen an. Wir haben daher das Resultat: ***Die Anzahl α aller positiven ambigen ursprünglichen Classen erster Art von negativer Determinante D ist halb so gross wie die Anzahl 2τ aller angebbaren Totalcharaktere.*** Dies gilt offenbar auch noch für den oben ausgeschlossenen singulären Fall $D = -1$, da die beiden Formen $(1, 0, 1)$, $(2, 1, 1)$ äquivalent sind.

Ist aber die Determinante D *positiv*, so entspricht jeder der obigen 2τ ambigen Formen (A, B, C) eine einzige ihr äquivalente ambige Form (A, B', C'), wo B' durch die Bedingungen

$$B' \equiv B \pmod{A}, \quad 0 < \sqrt{D} - B' < (A)$$

vollständig bestimmt ist; offenbar entstehen auf diese Weise wieder 2τ ambige und von einander verschiedene Formen (A, B', C'). Um nun zu zeigen, dass alle diese Formen zugleich *reducirt* sind (§. 74), braucht nur nachgewiesen zu werden, dass $(A) < \sqrt{D} + B'$ ist; wenn $(A) < \sqrt{D}$ ist, so folgt dies unmittelbar daraus, dass zufolge der obigen Grenzbedingungen B' positiv ist; wenn aber $(A) > \sqrt{D}$

ist, was nur bei den Formen des zweiten Typus eintreten kann, so ist $A = 2B$, und $(B) < \sqrt{D}$, folglich $B' = (B)$, weil dieser Werth allen an B' gestellten Forderungen genügt, und also wieder $(A) < \sqrt{D} + B'$. Endlich behaupten wir, dass jede ambige reducirte Form (a, b, c), welche zugleich ursprünglich von erster Art ist, nothwendig mit einer dieser 2τ Formen (A, B', C') identisch sein muss; ist nämlich b theilbar durch a, so muss $(a) < \sqrt{D}$ sein, weil in einer reducirten Form $0 < b < \sqrt{D}$ ist, und die mit (a, b, c) äquivalente Form $(a, 0, a')$ ist eine der 2τ Formen (A, B, C), woraus folgt, dass (a, b, c) selbst mit der entsprechenden Form (A, B', C') identisch sein muss, weil b als mittlerer Coefficient einer reducirten Form denselben charakteristischen Bedingungen genügt, wie B'; ist aber b nicht theilbar durch a, so ist wenigstens $(a) < 2\sqrt{D}$, und folglich die mit (a, b, c) äquivalente Form $(a, \frac{1}{2}a, c')$ eine der Formen (A, B, C), woraus wieder folgt, dass (a, b, c) mit der entsprechenden Form (A, B', C') identisch ist. Wir müssen aus dem Vorhergehenden schliessen, dass die Anzahl aller ambigen ursprünglichen Formen erster Art, welche zugleich reducirt sind, genau $= 2\tau$ ist; da nun in jeder ambigen Classe sich stets zwei und nur zwei solche Formen finden (§§. 78, 82), so erhalten wir dasselbe Resultat, wie für negative Determinanten: *Die Anzahl α aller ambigen ursprünglichen Classen erster Art von positiver Determinante D ist genau halb so gross wie die Anzahl 2τ aller angebbaren Totalcharaktere.*

Verbinden wir diese Resultate mit dem des vorigen Paragraphen, so ergiebt sich folgender Satz*):

Die Anzahl der wirklich existirenden verschiedenen Geschlechter ist höchstens halb so gross wie die Anzahl der angebbaren Totalcharaktere.

§. 154.

Das soeben erhaltene Resultat führt nun zu einem neuen Beweise des Reciprocitätssatzes, sowie der Ergänzungssätze über den Charakter der Zahlen -1 und 2. Wir machen zunächst die Be-

*) Vergl. §. 123.

merkung, dass in den Fällen $D = -1, \pm 2$, und wenn $D \equiv 1$ (mod. 4) eine positive oder negative Primzahl ist, nur ein einziger Charakter C (§. 122), und folglich (§. 153) nur ein einziges Geschlecht vorhanden ist, welches kein anderes, als das durch die Form $(1, 0, -D)$ vertretene Hauptgeschlecht $(C = +1)$ sein kann. Wir bezeichnen nun mit p, q immer positive, ungerade (von einander verschiedene) Primzahlen, und wenden uns zum Beweise der drei Sätze:

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{1}{2}(p-1)}, \quad \left(\frac{2}{p}\right) = (-1)^{\frac{1}{8}(p^2-1)}$$

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{1}{2}(p-1)\cdot\frac{1}{2}(q-1)}.$$

1. Ist zunächst $p \equiv 1$ (mod. 4), so ist $(-1, 0, p)$ eine ursprüngliche Form erster Art von der Determinante $D = p \equiv 1$ (mod. 4), für welche nur Formen existiren, die dem Hauptgeschlecht angehören; mithin muss der Coefficient -1 quadratischer Rest von p sein. Ist aber $p \equiv 3$ (mod. 4), so ist -1 Nichtrest von p; wäre nämlich $-1 = b^2 - cp$, so wäre (p, b, c) eine (positive) Form der Determinante $D = -1$, welche zufolge ihres Coefficienten p den Charakter $C = -1$ besässe, was unmöglich ist.

2. Ist $p \equiv 1$ (mod. 8), so ist $(8, 1, \frac{1}{8}(1-p))$ oder $(8, 3, \frac{1}{8}(9-p))$, je nachdem $p \equiv 9$ oder $\equiv 1$ (mod. 16) ist, eine ursprüngliche Form erster Art von der Determinante $D = p \equiv 1$ (mod. 4), und muss deshalb dem Hauptgeschlecht angehören, woraus folgt, dass 8 und also auch 2 quadratischer Rest von p ist.

Ist ferner $p \equiv 7$ (mod. 8), so ist 2 ebenfalls quadratischer Rest von p; denn im entgegengesetzten Fall wäre (zufolge 1. und §. 33, III.) die Zahl -2 Rest von p, also $-2 = b^2 - cp$, und es existirte eine (positive) Form (p, b, c) der Determinante $D = -2$, für welche $C = -1$ wäre, was unmöglich ist.

Ist endlich $p \equiv 3$ oder 5 (mod. 8), so ist 2 Nichtrest von p; wäre nämlich $2 = b^2 - cp$, so wäre (p, b, c) eine Form der Determinante $D = 2$, für welche $C = -1$ wäre, was unmöglich ist.

3. Ist wenigstens eine der beiden Primzahlen p, q, z. B. $p \equiv 1$ (mod. 4), so ist

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right).$$

Ist nämlich q Rest von p, so gilt Dasselbe von $-q$ (zufolge 1. und §. 33, I.), mithin kann man, nachdem man das Vorzeichen $\pm$ so gewählt hat, dass $\pm q \equiv 1 \pmod 4$ wird, immer $\pm q = b^2 - cp$ setzen, und folglich ist (p, b, c) eine ursprüngliche Form erster Art von der Determinante $D = \pm q \equiv 1 \pmod 4$, und zwar eine positive, wenn D negativ ist; sie gehört also dem Hauptgeschlechte an, und folglich ist p Rest von q. Ist aber q Nichtrest von p, so muss auch p Nichtrest von q sein, weil im entgegengesetzten Falle $p = b^2 - cq$ wäre, also eine ursprüngliche Form erster Art (q, b, c) der Determinante $D = p \equiv 1 \pmod 4$ existirte, für welche $C = -1$ wäre, was unmöglich ist.

Sind aber beide Primzahlen $p, q \equiv 3 \pmod 4$, so ist

$$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right).$$

Dies ergiebt sich am einfachsten durch die Betrachtung der Determinante $D = pq \equiv 1 \pmod 4$, für welche zwei Charaktere C, also höchstens zwei verschiedene Geschlechter existiren. Da nun die beiden ursprünglichen Formen $(1, 0, -pq)$, $(-1, 0, pq)$ erster Art (zufolge 1.) wirklich zwei verschiedenen Geschlechtern angehören, so muss jede andere ursprüngliche Form erster Art von derselben Determinante, z. B. die Form $(p, 0, -q)$ einem der durch diese beiden Formen repräsentirten Geschlechter angehören. Gehört sie in das Hauptgeschlecht, so ist gleichzeitig p Rest von q, und $-q$ Rest von p, folglich (nach 1.) q Nichtrest von p; gehört sie aber in dasselbe Geschlecht wie die Form $(-1, 0, pq)$, so ist gleichzeitig p Nichtrest von q, und $-q$ Nichtrest von p, folglich q Rest von p. Was zu beweisen war.

§. 155.

Mit Hülfe des so von Neuem bewiesenen Reciprocitätssatzes lässt sich nun wieder, wie in §. 123 geschehen ist, darthun, dass höchstens diejenigen τ Geschlechter existiren können, deren Totalcharaktere der dortigen Bedingung $\Pi C' = +1$ genügen; dass aber alle diese τ Geschlechter wirklich existiren (§. 125), hat *Gauss* mit Hülfe der von ihm gegründeten Theorie der ternären quadratischen Formen

$$Ax^2 + By^2 + Cz^2 + 2A'yz + 2B'zx + 2C'xy$$

bewiesen*). Da oben (§. 152) gezeigt ist, dass $ng = \alpha q$ ist, wo g die Anzahl der wirklich existirenden Geschlechter, n die Anzahl der in jedem derselben enthaltenen Classen, $\alpha = \tau$ die Anzahl der ambigen Classen oder also die Anzahl der Totalcharaktere, welche der Bedingung $\Pi C' = +1$ genügen, und q die Anzahl der durch Duplication entstehenden Classen bedeutet, so leuchtet ein, dass der zu beweisende Satz $g = \alpha$ wesentlich identisch ist mit dem Satze $n = q$; da ferner n die Anzahl aller Classen des Hauptgeschlechtes ist, und jede der durch Duplication entstehenden q Classen gewiss dem Hauptgeschlechte angehört (§. 152), so ist der zu beweisende Satz wesentlich identisch mit dem folgenden**):

Jede Classe des Hauptgeschlechtes entsteht durch Duplication.

Wir können hier unmöglich darauf eingehen, den Beweis mitzutheilen, welchen *Gauss* auf die Theorie der ternären Formen gestützt hat; da dieses tiefe Theorem aber den schönsten Abschluss der Lehre von der Composition bildet, so können wir es uns nicht versagen, dasselbe auch ohne Hülfe der Dirichlet'schen Principien auf einem Wege abzuleiten, der zugleich die Grundlage für andere wichtige Untersuchungen bildet.

Um einen bestimmten Boden für diese Untersuchung zu gewinnen, heben wir zunächst eine charakteristische Eigenschaft aller der Classen Q hervor, welche durch Duplication entstehen: *alle Formen dieser Classen und nur diese Formen sind fähig, Quadratzahlen darzustellen, welche relative Primzahlen zu $2D$ sind.* Entsteht nämlich Q durch Duplication einer Classe K, so kann man aus K immer eine solche Form auswählen, deren erster Coefficient x relative Primzahl zu $2D$ ist; da alsdann diese Form mit sich selbst einig ist, so entsteht durch Duplication eine der Classe Q angehörige Form, deren erster Coefficient $= x^2$ ist, und folglich ist diese Quadratzahl durch die Formen der Classe Q eigentlich darstellbar. Umgekehrt, ist Q eine Classe, durch deren Formen eine Quadratzahl dargestellt werden kann, welche relative Primzahl zu $2D$ ist, so giebt es auch eine solche Quadratzahl x^2, welche durch diese Formen *eigentlich* darstellbar ist, und folglich findet sich in dieser Classe Q eine Form (x^2, x', x''), welche offenbar

*) *D. A.* art. 287.

**) *Gauss: D. A.* art. 286.

durch Duplication der Form (x, x', xx'') entsteht; mithin ist $Q = K^2$, wo K die Classe bedeutet, welcher die Form (x, x', xx'') angehört. Das obige zu beweisende Theorem ist daher identisch mit dem folgenden:

Ist (A, B, C) eine Form des Hauptgeschlechtes der Determinante D, so ist die Gleichung

$$Az^2 + 2Bzy + Cy^2 = x^2$$

stets lösbar in ganzen Zahlen z, y, x, deren letzte relative Primzahl zu $2D$ ist.

§. 156.

Durch die vorstehende Betrachtung sind wir dahin geführt, die Lösbarkeit einer Gleichung von der Form

$$ax^2 + by^2 + cz^2 + 2a'yz + 2b'zx + 2c'xy = 0$$

in ganzen Zahlen x, y, z (oder was Dasselbe ist, die Lösbarkeit der allgemeinen Gleichung

$$au^2 + bv^2 + 2c'uv + 2b'u + 2a'v + c = 0$$

in *rationalen* Zahlen u, v) zu untersuchen. Dieselbe kann, allgemein zu reden, auf den speciellen Fall zurückgeführt werden, in welchem die Coefficienten $a', b', c' = 0$ sind*), und wir beschäftigen uns daher im Folgenden nur mit Gleichungen von der Form

$$ax^2 + by^2 + cz^2 = 0, \qquad (1)$$

wo a, b, c drei gegebene, von Null verschiedene ganze Zahlen bedeuten, die wir ausserdem stets als *relative Primzahlen* annehmen, weil jeder andere Fall, wie man leicht erkennt, sich auf diesen zurückführen lässt**). Wir wollen nun eine Lösung x, y, z eine *eigentliche* Lösung nennen, wenn die drei Zahlen x, y, z *relative Primzahlen* sind; dann leuchtet ein, dass ax, by, cz ebenfalls relative Primzahlen sind; ginge nämlich eine Primzahl p in zweien von ihnen auf, so müsste p zufolge (1) auch in der dritten aufgehen; da aber höchstens einer der Coefficienten a, b, c durch p

*) *Gauss: D. A.* artt. 299, 300.
**) *Gauss: D. A.* art. 298.

theilbar sein kann, so wären wenigstens zwei der Zahlen x, y, z theilbar durch p, also keine relative Primzahlen.

Nach dieser Vorbemerkung beginnen wir unsere Untersuchung*), indem wir uns die folgende Aufgabe stellen:

I. *Aus einer gegebenen eigentlichen Lösung* $x = u$, $y = v$, $z = w$ *der Gleichung* (1) *ihre sämmtlichen Lösungen abzuleiten.*

Da au, bv, cw relative Primzahlen sind, und eine von ihnen, z. B. au, zufolge der Gleichung

$$au^2 + bv^2 + cw^2 = 0 \tag{2}$$

gerade ist, so haben auch die Zahlen $2au$, bv, cw keinen gemeinschaftlichen Theiler, und man kann daher (nach §. 24) die Gleichung

$$aul + bvm + cwn = 1$$

so lösen, dass l gerade, und folglich die eine der beiden Zahlen m, n gerade, die andere ungerade wird; setzt man nun

$$al^2 + bm^2 + cn^2 = h$$

und

$$u' = 2l - hu,\ v' = 2m - hv,\ w' = 2n - hw,$$

so wird h ungerade, und man erhält**)

$$au'^2 + bv'^2 + cw'^2 = 0 \tag{3}$$

$$auu' + bvv' + cww' = 2 \tag{4}$$

$$u \equiv u',\ v \equiv v',\ w \equiv w' \pmod 2; \tag{5}$$

man kann daher

$$vw' - wv' = 2u'',\ wu' - uw' = 2v'',\ uv' - vu' = 2w'' \tag{6}$$

setzen, wo u'', v'', w'' ganze Zahlen bedeuten, welche mit den andern noch durch folgende Relationen***) verbunden sind:

---

*) Sie ist der Kürze halber synthetisch geführt; derselbe Gegenstand ist auf andere Weise behandelt in der mir erst nachträglich bekannt gewordenen Abhandlung von *G. Cantor: De aequationibus secundi gradus indeterminatis.* 1867.

**) Umgekehrt lässt sich aus (2), (3), (4), (5) leicht beweisen, dass a, b, c relative Primzahlen sind, und dass sowohl u, v, w, als auch u', v', w' eigentliche Lösungen der Gleichung (1) bilden; doch ist dies für unsere Zwecke nicht nöthig.

***) Man findet z. B. die erste der Gleichungen (7) aus der identischen Gleichung

$$(bv^2 + cw^2)(bv'^2 + cw'^2) = (bvv' + cww')^2 + bc(vw' - wv')^2$$

unter Berücksichtigung von (2), (3), (4), (6); die Gleichung (8) ergiebt sich

$$\left.\begin{aligned} auu' &= 1 + bcu''^2 \\ bvv' &= 1 + cav''^2 \\ cww' &= 1 + abw''^2 \end{aligned}\right\} \tag{7}$$

$$bcu''^2 + cav''^2 + abw''^2 = -1 \tag{8}$$

$$\left.\begin{aligned} vw' + wv' &= 2av''w'' \\ wu' + uw' &= 2bw''u'' \\ uv' + vu' &= 2cu''v'' \end{aligned}\right\} \tag{9}$$

Mit Hülfe derselben ist es leicht, unsere Aufgabe allgemein zu lösen. Sind x, y, z drei beliebige ganze Zahlen, so werden auch

$$\left.\begin{aligned} t &= au'x + bv'y + cw'z \\ t' &= aux + bvy + cwz \\ t'' &= u''x + v''y + w''z \end{aligned}\right\} \tag{10}$$

ganze Zahlen, welche zufolge (5) der Bedingung

$$t \equiv t' \pmod 2 \tag{11}$$

genügen; umgekehrt, sind t, t', t'' drei beliebige ganze Zahlen, welche nur der Bedingung (11) unterworfen sind, so folgt aus (10) unter Berücksichtigung von (5), (7) und (9), dass

$$\left.\begin{aligned} 2x &= ut + u't' - 2bcu''t'' \\ 2y &= vt + v't' - 2cav''t'' \\ 2z &= wt + w't' - 2abw''t'' \end{aligned}\right\} \tag{12}$$

gerade, also x, y, z ganze Zahlen sind. Multiplicirt man diese letzten Gleichungen resp. mit ax, by, cz, und addirt mit Rücksicht auf (10), so folgt

$$ax^2 + by^2 + cz^2 = tt' - abct''^2;$$

mithin haben wir folgendes Resultat: *Bilden die ganzen Zahlen x, y, z eine Lösung der Gleichung* (1), *so werden t, t', t'' vermöge* (10) *ganze Zahlen, welche den Bedingungen* (11) *und*

$$tt' = abct''^2 \tag{13}$$

genügen; umgekehrt, befriedigen die ganzen Zahlen t, t', t'' die Be-

---

durch Addition aus (7) mit Rücksicht auf (4); und die erste der Gleichungen (9) folgt aus der Identität

$$(auu' + bvv' + cww')(vw' + wv') - a(ww' - uw')(uv' - vu') = (au^2 + bv^2 + cw^2)v'w' + (au'^2 + bv'^2 + cw'^2)vw.$$

dingungen (11) *und* (13), *so werden* x, y, z *vermöge* (12) *ganze Zahlen, welche der Gleichung* (1) *genügen**).

Zur Vervollständigung fügen wir hinzu: *Damit die Zahlen* x, y, z *eine eigentliche Lösung der Gleichung* (1) *bilden, ist ferner erforderlich und hinreichend, dass die Zahlen* t, t' *keinen ungeraden gemeinschaftlichen Theiler haben, und dass, wenn beide gerade sind,*

$$t + t' \equiv 2 \pmod{4} \tag{14}$$

ist.

Für unsern Zweck genügt es zu beweisen, dass die beiden angegebenen Bedingungen hinreichend sind. Gesetzt, es ginge eine Primzahl p in zweien der Zahlen ax, by, cz auf, so müsste sie zufolge (1) auch in der dritten aufgehen, mithin zufolge (10) auch in t und t'; da aber t, t' der Annahme nach keinen ungeraden gemeinschaftlichen Theiler haben, so müsste $p = 2$ sein, und es wären also t, t', ax, by, cz gerade Zahlen; dann würde aber aus (10) mit Rücksicht auf (5) folgen, dass $t + t' \equiv 0 \pmod{4}$ wäre, während wir doch angenommen haben, dass $t + t' \equiv 2 \pmod{4}$ ist, sobald t und t' gerade Zahlen sind. Hieraus folgt also, dass ax, by, cz relative Primzahlen sind, was zu beweisen war**).

---

*) Die allgemeinste Lösung der Gleichung (13), deren wir zwar in der Folge nicht bedürfen, besteht, wie man sehr leicht findet, in den Gleichungen

$$t = \tau d \omega^2, \quad t' = \tau d' \omega'^2, \quad t'' = \tau \omega \omega',$$

wo d, d', τ, ω, ω' beliebige ganze Zahlen bedeuten, welche der einzigen Bedingung

$$d d' = abc$$

unterworfen sind; man kann aber auch, ohne die Allgemeinheit zu beeinträchtigen, annehmen, dass τ der grösste gemeinschaftliche Theiler von t, t', t'', und dass τd, $\tau d'$ die grössten Theiler sind, welche τabc resp. mit t, t' gemeinschaftlich hat. Führt man diese Ausdrücke in (12) ein, so erhält man die binären quadratischen Formen

$$\frac{2x}{\tau} = (du, -bcu'', d'u'), \quad \frac{2y}{\tau} = (dv, -cav'', d'v'),$$
$$\frac{2z}{\tau} = (dw, -abw'', d'w'),$$

deren Variabeln ω, ω', und deren Determinanten zufolge (7) die Zahlen $-bc$, $-ca$, $-ab$ sind. Transformirt man diejenige dieser Formen, deren Determinante negativ ist, in eine reducirte Form (§. 64), so erhält man die einfachsten Lösungen.

**) Es ist leicht, wenn auch für unsern Zweck nicht erforderlich, die beiden angegebenen Bedingungen auf die Zahlen d, d', τ, ω, ω' zu übertragen: die Zahlen d, d' müssen relative Primzahlen sein, und nur, wenn

II. Bilden die Zahlen x, y, z eine eigentliche Lösung der Gleichung (1), so sind ax, by, cz relative Primzahlen, und man kann folglich drei Zahlen $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$ bestimmen, welche den Congruenzen

$$\mathfrak{A}z \equiv by \pmod{a}, \quad \mathfrak{B}x \equiv cz \pmod{b}, \quad \mathfrak{C}y \equiv ax \pmod{c} \tag{15}$$

genügen, woraus in Verbindung mit (1)

$$\mathfrak{A}^2 \equiv -bc \pmod{a}, \quad \mathfrak{B}^2 \equiv -ca \pmod{b}, \quad \mathfrak{C}^2 \equiv -ab \pmod{c} \tag{16}$$

folgt. Wir haben mithin folgenden Satz erhalten:

Ist die Gleichung (1) *eigentlich lösbar, so sind die Zahlen* $-bc$, $-ca$, $-ab$ *resp. quadratische Reste der Zahlen* a, b, c, *und jede eigentliche Lösung* x, y, z *führt durch die Congruenzen* (15) *zu drei völlig bestimmten Zahlclassen* $\mathfrak{A}$ *(mod.* a*)*, $\mathfrak{B}$ *(mod.* b*)*, $\mathfrak{C}$ *(mod.* c*), welche den Congruenzen* (16) *genügen*).*

Von der grössten Wichtigkeit für unsere Untersuchungen ist es aber, dass dieser Satz sich in folgender Weise umkehren lässt:

Ist die Gleichung (1) *eigentlich lösbar, und sind drei Zahlen* $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$ *gegeben, welche den Congruenzen* (16) *genügen, so kann man stets eigentliche Lösungen* x, y, z *finden, welche die Bedingungen* (15) *erfüllen.*

Um dies zu beweisen, bestimmen wir zunächst drei Zahlen X, Y, Z durch die (nach §. 25) stets vereinbaren Congruenzpaare

$$\left.\begin{aligned} X &\equiv c \pmod{b}, \quad Y \equiv a \pmod{c}, \quad Z \equiv b \pmod{a} \\ X &\equiv \mathfrak{C} \pmod{c}, \quad Y \equiv \mathfrak{A} \pmod{a}, \quad Z \equiv \mathfrak{B} \pmod{b} \end{aligned}\right\} \tag{17}$$

aus welchen unter Berücksichtigung der Annahme (16) die der Gleichung (1) ähnliche Congruenz

$$aX^2 + bY^2 + cZ^2 \equiv 0 \pmod{abc} \tag{1'}$$

folgt, weil ihre linke Seite durch jede der drei relativen Primzahlen a, b, c theilbar ist. Da ferner die Existenz einer eigentlichen Lö-

---

$abc \equiv 0 \pmod 8$, können sie auch den grössten gemeinschaftlichen Theiler 2 haben; umgekehrt, genügt die Zerlegung $abc = dd'$ diesen Bedingungen, so kann man τ, ω, ω' so wählen, dass x, y, z eine eigentliche Lösung der Gleichung (1) bilden.

*) Wirft man zwei eigentliche Lösungen in dieselbe oder in verschiedene *Classen*, je nachdem sie zu denselben drei Zahlclassen $\mathfrak{A}$ (mod. a), $\mathfrak{B}$ (mod. b), $\mathfrak{C}$ (mod. c) führen oder nicht, so ist die Anzahl aller verschiedenen Classen *höchstens* gleich der Anzahl der incongruenten Wurzeln der Congruenz $x^2 \equiv 1 \pmod{abc}$, und der nachfolgende Satz behauptet die wirkliche Existenz aller dieser Classen von eigentlichen Lösungen.

sung u, v, w der Gleichung (1) angenommen ist, so behalten wir alle früheren Bezeichnungen bei und setzen

$$\left.\begin{aligned} T &\equiv au'X + bv'Y + cw'Z \\ T' &\equiv auX + bvY + cwZ \end{aligned}\right\} \text{(mod. } 2abc\text{)}, \qquad (10')$$

woraus zufolge (5)

$$T \equiv T' \text{ (mod. 2)} \qquad (11')$$

und mit Rücksicht auf (7) und (9)

$$\left.\begin{aligned} 2X &\equiv uT + u'T' \text{ (mod. } 2bc\text{)} \\ 2Y &\equiv vT + v'T' \text{ (mod. } 2ca\text{)} \\ 2Z &\equiv wT + w'T' \text{ (mod. } 2ab\text{)} \end{aligned}\right\} \qquad (12')$$

folgt; multiplicirt man diese Congruenzen resp. mit aX, bY, cZ, wodurch sie in Congruenzen nach dem Modulus $2abc$ übergehen, so ergiebt sich durch Addition unter Berücksichtigung von (1') und (10')

$$TT' \equiv 0 \text{ (mod. } abc\text{)}. \qquad (13')$$

Wir behaupten nun, dass die drei Zahlen T, T', abc keinen ungeraden gemeinschaftlichen Divisor haben, und dass, wenn abc gerade ist,

$$T + T' \equiv 2 \text{ (mod. 4)} \qquad (14')$$

ist. Ginge nämlich eine ungerade Primzahl p in T, T' und abc, also auch z. B. in c auf, so würde Y zufolge (12') durch p theilbar sein, und da $a \equiv Y$ (mod. c) ist, so hätten a und c den gemeinschaftlichen Theiler p, was unmöglich ist. Wenn ferner abc, und also auch z. B. c gerade ist, so sind zufolge (11') und (13') auch T und T' gerade Zahlen; wäre nun die Congruenz (14') unrichtig, so wäre $T' \equiv T$ (mod. 4), und aus (12') würde folgen, dass $2Y \equiv (v + v')T \equiv 0$ (mod. 4), also Y gerade wäre, was abermals gegen die Congruenz $a \equiv Y$ (mod. c) streitet, weil a relative Primzahl zu c ist.

Nach diesen Vorbereitungen sind wir im Stande, eine eigentliche Lösung x, y, z nachzuweisen, welche den Bedingungen (15) genügt; diese letztern gehen vermöge der Definition (17) der Zahlen X, Y, Z in die folgenden über

$$Yz \equiv Zy \text{ (mod. } a\text{)}, \quad Zx \equiv Xz \text{ (mod. } b\text{)}, \quad Xy \equiv Yx \text{ (mod. } c\text{)};$$

da ferner aus den Definitionen (10) und (10') der Zahlen t, t' T, T' die Congruenz

$$\left.\begin{array}{c} T't - Tt' \equiv \\ 2bcu''(Yz-Zy)+2cav''(Zx-Xz)+2abw''(Xy-Yx) \end{array}\right\} (\text{mod. } 2abc)$$

folgt, und da u'', v'', w'' zufolge (7) resp. relative Primzahlen zu a, b, c sind, so fallen die von x, y, z zu erfüllenden Bedingungen (15) durchaus mit der einzigen Forderung

$$T't \equiv Tt' \text{ (mod. } 2abc)$$

zusammen, welcher die Zahlen t, t' genügen müssen; sollen ferner die Zahlen x, y, z eine eigentliche Lösung der Gleichung (1) bilden, so haben t und t' ausserdem noch die früher erwähnten Bedingungen (11), (13), (14) zu erfüllen. Dies Alles lässt sich in der That auf folgende Weise erreichen.

Ist abc ungerade, so sei d der grösste gemeinschaftliche Theiler der beiden Zahlen T und $abc = dd'$; da nun zufolge (13') TT' durch abc theilbar ist, so geht d' in T' auf, und da, wie oben gezeigt ist, die Zahlen T, T', abc keinen ungeraden gemeinschaftlichen Theiler haben, so sind d und d' relative Primzahlen, und d' ist zugleich der grösste gemeinschaftliche Theiler der beiden Zahlen T' und abc. Dann leuchtet ein, dass man allen Forderungen genügt, wenn man z. B. $t = d$, $t' = d'$, $t'' = 1$ nimmt; denn weil $t \equiv t' \equiv 1$ (mod. 2), so werden x, y, z ganze Zahlen, die wegen $tt' = abct''^2$ eine Lösung der Gleichung (1) bilden; diese Lösung ist eine eigentliche, weil t, t' ungerade relative Primzahlen sind; da endlich $t \equiv t'$, $T \equiv T'$ (mod. 2), und $T't \equiv Tt' \equiv 0$ (mod. dd') ist, so folgt auch $T't \equiv Tt'$ (mod. $2abc$) d. h. die eigentliche Lösung x, y, z genügt den vorgeschriebenen Congruenzen (15).

Ist aber abc, und folglich auch T, T' gerade, und zwar $T + T' \equiv 2$ (mod. 4), so können wir der Symmetrie wegen annehmen, es sei $T \equiv 0$, $T' \equiv 2$ (mod. 4); dann sei d wieder der grösste gemeinschaftliche Theiler der beiden Zahlen T und $abc = dd'$, so wird d' in T' aufgehen. Ist nun d' ungerade, so genügt man allen Bedingungen, wenn man z. B. $t = 2d$, $t' = 2d'$, $t'' = 2$ nimmt; denn es ist $t \equiv 0$, $t' \equiv 2$ (mod. 4), $tt' = abct''^2$, $T't \equiv Tt' \equiv 0$ (mod. $2abc$), und t, t' haben keinen ungeraden gemeinschaftlichen Theiler. Ist aber d' gerade, so kann man wieder durch $t = d$, $t' = d'$, $t'' = 1$ allen Bedingungen genügen; da nämlich $T:d$ relative Primzahl zu d' und folglich ungerade ist, so muss, weil $T \equiv 0$ (mod. 4), auch $d \equiv 0$ (mod. 4) sein; da ferner d' in T' aufgeht, und $T' \equiv 2$ (mod. 4) ist, so muss auch $d' \equiv 2$ (mod. 4) sein; mithin ist $t \equiv 0$, $t' \equiv 2$ (mod. 4); es ist ferner $tt' = abct''^2$, und

die Zahlen t, t' haben keinen ungeraden gemeinschaftlichen Theiler; da endlich die Quotienten $T:d$ und $T':d'$ ungerade sind, so ist ihre Differenz gerade, und folglich, wenn man mit $dd' = abc$ multiplicirt, $Td' - T'd = Tt' - T't \equiv 0 \pmod{2abc}$, was zu beweisen war.

Es hat keine Schwierigkeit, ausser den eben angegebenen speciellen Lösungen, welche die vorgeschriebenen Congruenzen (15) erfüllen, alle andern zu bestimmen, und man findet namentlich leicht, dass zwei eigentliche Lösungen x, y, z und x_1, y_1, z_1, welche resp. durch die Werthe t, t', t'' und t_1, t_1', t_1'' hervorgebracht werden, stets und nur dann denselben Congruenzen (15) genügen, wenn $tt_1' \equiv t't_1 \pmod{2abc}$ ist*); allein alle diese an sich interessanten Vervollständigungen sind für unsere Zwecke nicht erforderlich. Wir begnügen uns daher, aus den obigen Resultaten noch den Beweis des folgenden Satzes abzuleiten, dessen wir später durchaus bedürfen.

III. *Ist die Gleichung* (1) *eigentlich lösbar, und ist* $-bc$ *quadratischer Rest von* ap^2, *wo* p *eine in* bc *nicht aufgehende Primzahl bedeutet, so besitzt die Gleichung* (1) *auch solche eigentliche Lösungen* x, y, z, *welche der Bedingung* $x \equiv 0$ (*mod.* p) *genügen.*

Der Annahme zufolge besitzt die Gleichung (1) eine eigentliche Lösung u, v, w, und wir können alle hieraus in I. gezogenen Folgerungen für uns in Anspruch nehmen; es versteht sich von selbst, dass wir den vorstehenden Satz nur für den Fall zu beweisen brauchen, dass keine der beiden Zahlen u, u' durch p theilbar ist.

Ist nun p ungerade, so kann man, da der Annahme nach $-bc \equiv \alpha^2 \pmod{p}$ ist, das Vorzeichen von α so wählen, dass $bcu'' + \alpha$ nicht theilbar durch p ist; wären nämlich beide Zahlen

*) Hieraus folgt, dass allen zu derselben Classe gehörigen eigentlichen Lösungen dieselbe Zerlegung $abc = dd'$ entspricht, mit einziger Ausnahme des Falles, wo $abc \equiv 2 \pmod{4}$, in welchem der Factor 2 nach Belieben in d oder in d' aufgenommen werden kann, ohne dass eine Aenderung der Classe eintritt. Auf diese Weise ergiebt sich (vergl. die früheren Noten), dass die Anzahl der wesentlich verschiedenen Zerlegungen, und also auch die der wirklich existirenden Classen genau mit der Anzahl der incongruenten Wurzeln der Congruenz $x^2 \equiv 1 \pmod{abc}$ übereinstimmt; hierin liegt also ein neuer Beweis des obigen Satzes. Aber es schien angemessener, ihn so zu führen, dass zugleich eine Lösung gefunden wird, welche den vorgeschriebenen Congruenzen genügt.

$bcu'' + \alpha$ und $bcu'' - \alpha$ durch p theilbar, so müsste auch ihre Differenz 2α, also auch α durch die ungerade Primzahl p theilbar sein, was gegen $-bc \equiv \alpha^2 \pmod{p}$ und die Annahme streitet, dass p nicht in bc aufgeht. Da nun u ebenfalls nicht durch p theilbar ist, so kann man eine Zahl ω stets so bestimmen (§. 25), dass sie der Congruenz

$$u\omega \equiv bcu'' + \alpha \pmod{p}$$

genügt und ausserdem relative Primzahl zu $2abc$ wird, weil ω, falls p in $2abc$, also in a aufgehen sollte, schon vermöge dieser Congruenz relative Primzahl zu p wird. Setzt man nun

$$t = \tau\omega^2, \quad t' = \tau abc, \quad t'' = \tau\omega,$$

wo $\tau = 1$ oder $= 2$ zu nehmen ist, je nachdem abc ungerade oder gerade ist, so erhält man eine entsprechende eigentliche Lösung x, y, z, welche auch der Bedingung $x \equiv 0 \pmod{p}$ genügt. Ist nämlich abc ungerade, also $\tau = 1$, so ist $t \equiv t' \equiv 1 \pmod{2}$; ist aber abc gerade, also $\tau = 2$, so ist $t \equiv 2$, $t' \equiv 0 \pmod{4}$; da ferner ω relative Primzahl zu abc ist, so haben t, t' keinen ungeraden gemeinschaftlichen Divisor, und da $tt' = abct''^2$ ist, so bilden x, y, z eine eigentliche Lösung der Gleichung (1). Nun ist nach (12)

$$\begin{aligned} 2x &= ut + u't' - 2bcu''t'' \\ &= \tau(u\omega^2 - 2bcu''\omega + abcu') \end{aligned}$$

also mit Rücksicht auf (7)

$$2ux = \tau\{(u\omega - bcu'')^2 + bc\} \equiv 0 \pmod{p},$$

weil $u\omega - bcu'' \equiv \alpha$, $bc \equiv -\alpha^2$ ist; da endlich $2u$ nicht durch p theilbar ist, so folgt hieraus $x \equiv 0 \pmod{p}$.

Wir gehen jetzt zu dem Falle $p = 2$ über. Ist erstens a gerade, aber nicht $\equiv 0 \pmod{8}$, so ergiebt sich leicht, da der Annahme nach $-bc$ quadratischer Rest von $4a$, also $bc \equiv -1 \pmod{8}$ ist, dass u gar nicht ungerade sein kann; da nämlich a gerade, also bv, cw ungerade sind, und $b \equiv -c \pmod{8}$ ist, so folgt aus $au^2 + bv^2 + cw^2 = 0$, dass $au^2 \equiv 0 \pmod{8}$, und folglich, da a nicht $\equiv 0 \pmod{8}$ ist, jedenfalls u gerade sein muss; und offenbar haben dann alle anderen eigentlichen Auflösungen x, y, z dieselbe Eigenschaft $x \equiv 0 \pmod{2}$. Ist zweitens $a \equiv 0 \pmod{8}$, also $-bc \equiv 1 \pmod{8}$, so nehme man $t'' = 1$, und $tt' = abc$ der Art, dass einer der beiden Factoren, z. B. $t \equiv 2 \pmod{4}$, also der andere $t' \equiv 0 \pmod{4}$ wird, und dass sie keinen ungeraden gemeinschaftlichen Divisor erhalten, was sich stets erreichen lässt.

Hieraus folgt, dass die Zahlen x, y, z eine eigentliche Lösung bilden werden. Da nun der Voraussetzung nach u ungerade ist, und da aus $1 + bcu''^2 = auu' \equiv 0 \pmod 8$ folgt, dass auch u'' ungerade ist, so ergiebt sich

$$2x = ut + u't' - 2bcu''t'' \equiv 2 + 0 - 2 \equiv 0 \pmod 4,$$

also ist $x \equiv 0 \pmod 2$. Ist endlich drittens a ungerade, und $-bc$ quadratischer Rest von $4a$, also $bc \equiv -1 \pmod 4$, so nehme man $t'' = 1$, und nach Belieben $tt' = abc$, nur so, dass t und t' relative Primzahlen werden; dann bilden x, y, z eine eigentliche Lösung, weil ausserdem $t \equiv t' \equiv 1 \pmod 2$ ist. Da nun der Voraussetzung nach keine der Zahlen u, u' gerade ist, so folgt aus $auu' = 1 + bcu''^2$, dass u'' gerade, und folglich $auu' \equiv 1 \pmod 4$ ist; mithin ist $ut \cdot u't' = auu' \cdot bc \equiv -1 \pmod 4$, also $ut \equiv -u't' \pmod 4$, und hieraus ergiebt sich

$$2x = ut + u't' - 2bcu''t'' \equiv 0 \pmod 4,$$

also ist $x \equiv 0 \pmod 2$.

Hiermit ist der obige Satz vollständig bewiesen, und dieser Beweis enthält offenbar eine Methode, aus einer eigentlichen Lösung u, v, w einer Gleichung, deren Coefficienten a, b, c sind, eine eigentliche Lösung $x:p$, y, z derjenigen Gleichung abzuleiten, deren Coefficienten ap^2, b, c sind, vorausgesetzt, dass $-bc$ quadratischer Rest von ap^2 und nicht durch die Primzahl p theilbar ist. Durch wiederholte Anwendung desselben Satzes gelangt man offenbar zu folgendem Resultat:

Sind die Zahlen $A = aP^2$, $B = bQ^2$, $C = cR^2$ relative Primzahlen, und sind die Zahlen $-BC$, $-CA$, $-AB$ resp. quadratische Reste von A, B, C, so folgt aus der Existenz einer eigentlichen Lösung der Gleichung

$$ax^2 + by^2 + cz^2 = 0$$

stets die Existenz einer eigentlichen Lösung der Gleichung

$$Ax^2 + By^2 + Cz^2 = 0.$$

§. 157.

Durch den zuletzt bewiesenen Satz ist offenbar die Frage nach der eigentlichen Lösbarkeit der Gleichung

$$ax^2 + by^2 + cz^2 = 0 \qquad (1)$$

auf den Fall zurückgeführt, in welchem keine der relativen Primzahlen a, b, c durch ein Quadrat theilbar ist; als eine erforderliche Bedingung für die Lösbarkeit ist ferner im vorigen Paragraphen (II) erkannt, dass die Zahlen $-bc$, $-ca$, $-ab$ resp. quadratische Reste von den Zahlen a, b, c sein müssen, und ausserdem leuchtet ein, dass die letzteren unmöglich alle dasselbe Vorzeichen haben können. Mit Hülfe einer Reductionsmethode, welche im Wesentlichen von *Lagrange**) herrührt, lässt sich nun wirklich beweisen, dass diese Bedingungen auch die hinreichenden sind, dass also folgender Satz**) besteht:

Sind a, b, c drei von Null verschiedene und durch kein Quadrat theilbare relative Primzahlen, welche nicht alle dasselbe Vorzeichen haben, und sind die Zahlen $-bc$, $-ca$, $-ab$ resp. quadratische Reste der Zahlen a, b, c; so ist die Gleichung (1) *eigentlich lösbar.*

Zunächst bemerken wir, dass der Satz in dem speciellen Falle richtig ist, wenn einer der Coefficienten, z. B. $a = +1$, ein anderer, z. B. $b = -1$ ist; denn man genügt der Gleichung (1) durch die relativen Primzahlen $x = y = 1$, $z = 0$.

Um uns nun bequemer ausdrücken zu können, nennen wir, indem wir den absoluten Werth einer Grösse k mit (k) bezeichnen, dasjenige der drei Producte (bc), (ca), (ab), welches der Grösse nach zwischen den beiden anderen liegt, den *Index* der Gleichung (1), und wenn etwa zwei dieser Producte oder alle drei einander gleich sein sollten, so soll unter dem Index der gemeinschaftliche

---

*) *Sur la solution des problèmes indéterminés du second degré.* Mém. de l'Acad. de Berlin. T. XXIII. 1769. (Œuvres de L. T. II. 1868. p. 375.) — *Additions aux Élémens d'Algèbre par L. Euler.* §. V.

**) *Legendre: Théorie des Nombres,* 3me éd. T. I. §§. III, IV. — *Gauss: D. A.* artt. 294, 295. — Der nachfolgende Beweis lässt sich auf den Fall ausdehnen, dass a, b, c quadratische Divisoren besitzen.

Werth dieser beiden oder aller Producte verstanden werden. Aus dieser Erklärung ergiebt sich unmittelbar die Richtigkeit des Satzes für den Fall, dass ihr Index $= 1$ ist; denn dann muss, wie man leicht erkennt, $(a) = (b) = (c) = 1$ sein, und da die Coefficienten nicht alle dasselbe Vorzeichen haben, so ergiebt sich die Lösbarkeit der Gleichung aus der vorausgeschickten Bemerkung.

Um nun den Beweis allgemein zu führen, nehmen wir an, er sei schon geleistet für alle Gleichungen, deren Index kleiner als eine bestimmte positive ganze Zahl J ist, und zeigen, dass der Satz dann auch für alle Gleichungen gelten muss, deren Index $= J$ ist. Gelingt dies, so gilt der Satz allgemein, weil er für $J = 1$ richtig ist.

Es sei daher $J \geqq 2$ der Index der Gleichung (1). Nehmen wir an, was der Symmetrie wegen erlaubt ist, es sei $(a) \leqq (b) \leqq (c)$, also auch $(ab) \leqq (ac) \leqq (bc)$, so ist $J = (ac)$; wäre nun $(b) = (c)$, so müsste, weil b und c relative Primzahlen sind, $(b) = (c) = 1$ sein, woraus auch $J = 1$ folgen würde, was mit unserer Annahme streitet; mithin ist

$$(a) \leqq (b) < (c),\ (ab) < (ac) = J \leqq (bc). \tag{2}$$

Der Annahme nach ist nun $-ab$ quadratischer Rest von c, und folglich kann man eine Zahl r so bestimmen, dass $ar^2 \equiv -b \pmod{c}$, und zugleich $(r) \leqq \frac{1}{2}(c)$ wird; setzt man dann

$$ar^2 + b = cC, \tag{3}$$

so wird C eine ganze Zahl, deren absoluter Werth

$$(C) \leqq \frac{(a)r^2 + (b)}{(c)} < \tfrac{1}{4}J + 1 < J \tag{4}$$

ist, weil $(r) \leqq \frac{1}{2}(c)$, $(ac) = J \geqq 2$, und $(b) < (c)$ ist.

Ist nun $C = 0$, so folgt $b = -ar^2$, also, da b relative Primzahl zu a und durch kein Quadrat theilbar ist, $(r) = 1$ und $b = -a = \pm 1$, und mithin besitzt die Gleichung (1) in diesem Fall wieder die eigentliche Lösung $x = y = 1$, $z = 0$.

Ist aber C von Null verschieden, so führen wir die Gleichung (1) folgendermaassen auf eine andere von kleinerem Index zurück. Es sei a' der grösste gemeinschaftliche Divisor der drei in der Gleichung (3) vorkommenden Glieder ar^2, b, cC, so ist a' zugleich der grösste gemeinschaftliche Divisor von je zweien dieser Zahlen, so dass die drei Glieder der Gleichung

$$\frac{ar^2}{a'} + \frac{b}{a'} = \frac{cC}{a'}$$

gewiss relative Primzahlen sind. Da nun a' in b aufgeht, also relative Primzahl zu c und zu a ist, so muss a' in C und in r^2, also auch in r selbst aufgehen, weil a' als Divisor von b durch kein Quadrat theilbar ist. Man kann daher

$$r = a'\alpha, \quad b = a'\beta, \quad C = a'C' = a'c'\gamma^2 \tag{5}$$

setzen, wo γ^2 das grösste in $C' = c'\gamma^2$ aufgehende Quadrat bedeutet; hierdurch geht die Gleichung (3) in die folgende über

$$aa'\alpha^2 + \beta = cc'\gamma^2, \tag{6}$$

deren drei Glieder also relative Primzahlen sind; setzen wir endlich noch

$$b' = a\beta, \tag{7}$$

so sind hierdurch drei Zahlen a', b', c' definirt, welche, wie wir beweisen wollen, dieselben Eigenschaften besitzen, wie die gegebenen Zahlen a, b, c.

Dass erstens keine der Zahlen a', b', $c' = 0$ ist, leuchtet ein, weil $a'b' = a'a\beta = ab$ ist, und c' in C aufgeht. Aus $a'b' = ab$ folgt ferner, dass a', b' relative Primzahlen und durch kein Quadrat theilbar sind, weil a, b dieselben Eigenschaften haben; da ferner γ^2 das grösste in $C' = c'\gamma^2$ aufgehende Quadrat ist, so kann c' durch kein Quadrat theilbar sein; und da die Glieder der Gleichung (6) relative Primzahlen sind, so ist c' auch relative Primzahl zu $aa'\beta = a'b'$.

Die Zahlen a', b', c' können auch nicht alle dasselbe Vorzeichen haben; ist nämlich $ab = a'b'$ negativ, so haben a', b' entgegengesetzte Zeichen; ist aber ab positiv, folglich ca und bc negativ, so ergiebt sich aus der Gleichung $ar^2 + b = ca'c'\gamma^2$, dass $a'c'$ negativ ist, dass also a', c' entgegengesetzte Vorzeichen haben.

Da ferner zufolge der Gleichung (6), deren drei Glieder relative Primzahlen sind, die drei Zahlen $\beta cc'$, $aca'c'$, $-aa'\beta = -a'b'$ resp. quadratische Reste der drei Zahlen aa', β, c' sein müssen, und da nach Voraussetzung die beiden Zahlen $-bc = -\beta a'c$, $-ca$ resp. Reste von den beiden Zahlen a, $b = a'\beta$ sind, so ergiebt sich hieraus leicht, dass die drei Zahlen $-b'c'$, $-c'a'$, $-a'b'$ resp. Reste der drei Zahlen a', b', c' sind.

Endlich ist $(a'b') = (ab) < J$ zufolge (2), und $(c'a') \leqq (c'a')\gamma^2 = (C) < J$ zufolge (4); mithin ist der Index der Gleichung

$$a'x'^2 + b'y'^2 + c'z'^2 = 0$$

gewiss kleiner als J, und folglich ist sie nach unserer obigen Voraussetzung lösbar in relativen Primzahlen x', y', z'; da nun die Zahlen $a'\alpha x' - \beta y'$, $x' + a\alpha y'$ nicht beide verschwinden, weil sonst auch $x' = y' = 0$ wäre, so kann man

$$mx = a'\alpha x' - \beta y'; \quad my = x' + a\alpha y'; \quad mz = c'\gamma z'$$

setzen, wo m den grössten gemeinschaftlichen Theiler der drei Zahlen rechter Hand bedeutet; hieraus folgt aber mit Beachtung von (5), (6), (7)

$$m^2(ax^2 + by^2 + cz^2) = cc'\gamma^2(a'x'^2 + b'y'^2 + c'z'^2) = 0,$$

also, da m nicht $= 0$ ist, auch

$$ax^2 + by^2 + cz^2 = 0;$$

da endlich die Zahlen x, y, z keinen gemeinschaftlichen Theiler haben, und keine der Zahlen a, b, c durch ein Quadrat theilbar ist, so sind x, y, z auch relative Primzahlen und bilden folglich eine eigentliche Lösung der Gleichung (1).

Hiermit ist der Schluss vollständig durchgeführt, und also auch der obige Satz allgemein bewiesen. Es leuchtet ferner ein, dass in der successiven Zurückführung der Gleichung (1) auf ähnliche Gleichungen von immer kleinerem Index und endlich auf eine Gleichung, in welcher ein Coefficient $= +1$, ein anderer $= -1$ ist, auch eine Methode liegt, eine Lösung derselben zu finden.

Nachdem für diejenigen Gleichungen, deren Coefficienten durch kein Quadrat theilbar sind, die oben genannten *erforderlichen* Bedingungen zugleich als *hinreichend* für die Existenz eigentlicher Lösungen erkannt sind, so geht aus dem Schlusssatze des vorigen Paragraphen hervor, dass genau Dasselbe Statt findet für alle Gleichungen (1), deren Coefficienten von Null verschieden und relative Primzahlen sind. Wir können daher das Gesammtresultat unserer Untersuchungen in dem folgenden wichtigen Satze niederlegen:

Sind die Zahlen a, b, c relative Primzahlen und von Null verschieden, so ist die Gleichung

$$ax^2 + by^2 + cz^2 = 0$$

stets und nur dann in relativen Primzahlen x, y, z lösbar, wenn die Zahlen $-bc$, $-ca$, $-ab$ resp. quadratische Reste von den Zahlen a, b, c sind, und diese letzteren nicht alle dasselbe Vorzeichen haben; ist ferner

$-bc \equiv \mathfrak{A}^2 \pmod{a}$, $-ca \equiv \mathfrak{B}^2 \pmod{b}$, $-ab \equiv \mathfrak{C}^2 \pmod{c}$, *so ist die obige Gleichung in relativen Primzahlen* x, y, z *der Art lösbar, dass*

$\mathfrak{A}z \equiv by \pmod{a}$, $\mathfrak{B}x \equiv cz \pmod{b}$, $\mathfrak{C}y \equiv ax \pmod{c}$ *wird.*

§. 158.

Mit Hülfe dieses Satzes lässt sich nun das oben (§. 155) erwähnte grosse Theorem von *Gauss* leicht beweisen:

Jede Classe des Hauptgeschlechtes entsteht durch Duplication.

Als Repräsentanten der dem Hauptgeschlechte der Determinante D angehörenden Classe wählen wir eine Form (A, B, C), deren erster Coefficient A relative Primzahl zu $2D$ ist (§. 93). Da die Zahl A durch diese Form darstellbar ist, und alle Einzel-Charaktere derselben den Werth $+1$ haben, so ist A quadratischer Rest von jeder in D aufgehenden ungeraden Primzahl, und auch von 4 oder von 8, falls D durch 4 oder 8 theilbar ist (§. 122); mithin ist (nach §. 37) A quadratischer Rest von D selbst (umgekehrt ergiebt sich leicht, zum Theil mit Hülfe des Reciprocitätssatzes, dass die Form (A, B, C) gewiss dem Hauptgeschlecht angehört, wenn A relative Primzahl zu $2D$, quadratischer Rest von D, und, falls D negativ sein sollte, positiv ist). Ja, man kann sogar voraussetzen, dass A quadratischer Rest von $4D$ ist, d. h. dass $A \equiv 1 \pmod 4$, oder $A \equiv 1 \pmod 8$ ist, je nachdem D ungerade oder gerade ist. Dies ist in der That von selbst der Fall, wenn $D \equiv 3 \pmod 4$, oder $D \equiv 0 \pmod 8$ ist; sollte ferner A in den übrigen Fällen dieser Bedingung nicht genügen, wäre also $A \equiv 3 \pmod 4$, $\equiv 7 \pmod 8$, $\equiv 3 \pmod 8$, $\equiv 5 \pmod 8$, je nachdem $D \equiv 1 \pmod 4$, $\equiv 2 \pmod 8$, $\equiv 6 \pmod 8$, $\equiv 4 \pmod 8$, so kann man die Form (A, B, C) durch eine Substitution $\left(\begin{smallmatrix} \alpha, & -1 \\ 1, & 0 \end{smallmatrix}\right)$ in eine Form transformiren, deren erster Coefficient $A' = A\alpha^2 + 2B\alpha + C$ relative Primzahl zu $2D$ ist und zugleich die verlangte Eigenschaft besitzt; da nämlich $AA' = (A\alpha + B)^2 - D$ ist, so braucht man α nur so zu wählen, dass $A\alpha + B$ im ersten Falle gerade, in den drei übrigen Fällen aber ungerade wird, was sich stets in der Art erreichen lässt, dass $A\alpha + B$ zugleich relative Primzahl zu D wird.

Wir setzen daher voraus, dass A quadratischer Rest von $4D$ und relative Primzahl zu $4D$ ist; da nun $4D \equiv (2B)^2 \pmod{A}$, also quadratischer Rest von A ist, und da die Zahlen A, $4D$ nicht beide negativ sind, so besitzt die Gleichung

$$Ax^2 + 4Dy^2 - z^2 = 0$$

immer eigentliche Lösungen x, y, z, welche der Bedingung

$$2Bz \equiv 4Dy, \quad \text{also} \quad z \equiv 2By \pmod{A}$$

genügen (§. 157); man kann daher $z = At + 2By$ setzen, wodurch die obige Gleichung in die folgende übergeht

$$At^2 + 2B(2y) + C(2y)^2 = x^2;$$

da Ax, $2Dy$, z relative Primzahlen sind, so sind auch t, $2y$ relative Primzahlen, und folglich ist (A, B, C) einer Form äquivalent (§. 60), deren erster Coefficient x^2 eine Quadratzahl und relative Primzahl zu $2D$ ist, und welche folglich (nach §. 155) durch Duplication einer Form entsteht, deren erster Coefficient $\pm x$ ist. Was zu beweisen war*).

Die unendlich vielen eigentlichen Lösungen x, y, z der obigen Gleichung, welche der Bedingung $z \equiv 2By \pmod{A}$ genügen, zerfallen nun noch in verschiedene Classen in Bezug auf den Modul $4D$ (§. 156. II.); auf den Zusammenhang dieser Lösungen mit den verschiedenen Classen, durch deren Duplication dieselbe gegebene Classe des Hauptgeschlechtes entsteht, können wir aber hier nicht mehr eingehen.

§. 159.

Die Theorie der binären quadratischen Formen, ihrer Aequivalenz und Composition bildet nur einen speciellen Fall von der Theorie derjenigen homogenen Formen $n$ten Grades mit n Veränderlichen, welche sich in lineare Factoren mit algebraischen

*) Die Zurückführung dieses Satzes von *Gauss* auf den von *Lagrange* und *Legendre* ist, wie ich jetzt nachträglich bemerke, zuerst von *Arndt* ausgeführt (*Ueber die Anzahl der Genera der quadratischen Formen*; Crelle's Journal LVI), doch weicht die obige Darstellung in mehreren Puncten von der seinigen ab. In Wahrheit gehört der Satz von *Lagrange* nach Inhalt und Methode des Beweises in die Theorie der ternären Formen. — Man vergl. ferner *Kronecker: Ueber den Gebrauch der Dirichlet'schen Methoden in der Theorie der quadratischen Formen* (Monatsber. d. Berliner Ak. 12. Mai 1864).

Coefficienten zerlegen lassen. Diese Formen sind zuerst von *Lagrange**) betrachtet; später hat *Dirichlet***) sich vielfach mit diesem Gegenstande beschäftigt, aber er hat von seinen weit gehenden Untersuchungen nur diejenige veröffentlicht, welche die Transformationen solcher Formen in sich selbst (vergl. §§. 61, 62) oder, was dasselbe ist, die Theorie der Einheiten für die entsprechenden algebraischen Zahlen behandelt; endlich hat *Kummer****) durch die Schöpfung der idealen Zahlen einen neuen Weg betreten, welcher nicht nur zu einer sehr bequemen Ausdrucksweise, sondern auch zu einer tieferen Einsicht in die wahre Natur der algebraischen Zahlen führt. Indem wir versuchen, den Leser in diese neuen Ideen einzuführen, stellen wir uns auf einen etwas höheren Standpunct und beginnen damit, einen Begriff einzuführen, welcher wohl geeignet scheint, als Grundlage für die höhere Algebra und die mit ihr zusammenhängenden Theile der Zahlentheorie zu dienen.

I. Unter einem *Körper* wollen wir jedes System von unendlich vielen reellen oder complexen Zahlen verstehen, welches in sich so abgeschlossen und vollständig ist, dass die Addition, Subtraction, Multiplication und Division von je zwei dieser Zahlen immer wieder eine Zahl desselben Systems hervorbringt. Der einfachste Körper wird durch alle rationalen, der grösste Körper durch alle Zahlen gebildet. Wir nennen einen Körper A einen *Divisor* des Körpers M, diesen ein *Multiplum* von jenem, wenn alle in A enthaltenen Zahlen sich auch in M vorfinden; man findet leicht, dass der Körper der rationalen Zahlen ein Divisor von jedem andern Körper ist. Der Inbegriff aller Zahlen, welche gleichzeitig in zwei Körpern A, B enthalten sind, bildet wieder einen Körper D, welcher der *grösste* gemeinschaftliche Divisor der beiden Körper A, B genannt werden kann, weil offenbar jeder gemeinschaftliche Divisor von A und B nothwendig ein Divisor von D ist; ebenso existirt immer ein Körper M, welcher das *kleinste* gemeinschaftliche Multiplum von A und B heissen soll, weil er ein Divisor von jedem andern gemeinschaftlichen Multiplum der beiden Körper ist. Entspricht ferner einer jeden Zahl a des Körpers A eine Zahl $b = \varphi(a)$

---

*) *Sur la solution des problèmes indéterminés du second degré.* §. VI. Mém. de l'Ac. de Berlin. T. XXIII, 1769. (Œuvres de L. T. II, 1868, p. 375.) — *Additions aux Élémens d'Algèbre par L. Euler.* §. IX.

**) Vergl. Anm. zu §. 141.

***) Vergl. Anm. zu §. 16.

in der Weise, dass $\varphi(a+a') = \varphi(a) + \varphi(a')$, und $\varphi(aa') = \varphi(a)\,\varphi(a')$ ist, so bilden die Zahlen b (falls sie nicht sämmtlich verschwinden) ebenfalls einen Körper $B = \varphi(A)$, welcher *mit A conjugirt* ist und durch die *Substitution* φ aus A hervorgeht; dann ist rückwärts auch $A = \psi(B)$ mit B conjugirt. Zwei mit einem dritten conjugirte Körper sind auch mit einander conjugirt, und jeder Körper ist mit sich selbst conjugirt. Correspondirende Zahlen in zwei conjugirten Körpern A und B, wie a und $b = \varphi(a)$, sollen *conjugirte Zahlen* heissen.

Die einfachsten Körper sind diejenigen, welche nur eine *endliche* Anzahl von Divisoren besitzen. Nennt man m bestimmte Zahlen $\alpha_1, \alpha_2 \ldots \alpha_m$ *von einander abhängig* oder *unabhängig*, je nachdem die Gleichung $x_1\alpha_1 + x_2\alpha_2 + \cdots + x_m\alpha_m = 0$ in rationalen Zahlen $x_1, x_2 \ldots x_m$, die nicht sämmtlich verschwinden, lösbar ist oder nicht, so findet man durch sehr einfache Betrachtungen, auf die wir aber hier nicht eingehen wollen, dass aus einem Körper Ω von der angegebenen Art*) nur eine *endliche* Anzahl n von unabhängigen Zahlen $\omega_1, \omega_2 \ldots \omega_n$ sich auswählen lässt, dass also jede Zahl ω des Körpers stets und nur auf eine einzige Art durch die Form

$$\omega = h_1\omega_1 + h_2\omega_2 + \cdots + h_n\omega_n = \sum h_\iota\omega_\iota \qquad (1)$$

darstellbar ist, wo $h_1, h_2 \ldots h_n$ *rationale Zahlen* bedeuten. Wir wollen die Zahl n den *Grad*, ferner den Complex der n unabhängigen Zahlen ω_ι eine *Basis des Körpers* Ω, und die n Zahlen h_ι die dieser Basis entsprechenden *Coordinaten der Zahl* ω nennen; offenbar bilden je n Zahlen von der Form (1) wieder eine solche Basis, wenn die aus den entsprechenden n^2 Coordinaten gebildete Determinante von Null verschieden ist; einer solchen *Transformation* der Basis durch eine lineare Substitution entspricht eine Transformation der Coordinaten durch die sogenannte *transponirte* Substitution.

Die Forderung, dass die Zahlen ω des Körpers Ω durch Addition und Subtraction sich reproduciren sollen, wird durch ihre gemeinsame Form (1) schon erfüllt; für die Reproduction durch Multiplication ist ferner erforderlich und hinreichend, dass jedes

*) Ersetzt man die rationalen Zahlen überall durch Zahlen eines Körpers R, so gelten die nachfolgenden Betrachtungen auch für einen Körper Ω, welcher nur eine endliche Anzahl solcher Divisoren besitzt, die zugleich Multipla von R sind.

Product $\omega_\iota \omega_{\iota'}$ wieder in der Form (1) enthalten ist; diese Bedingungen, deren Anzahl $= \frac{1}{2}n(n+1)$ ist, lassen sich am einfachsten zusammenfassen, indem man die Coordinaten h_ι als *veränderlich* ansieht und

$$\omega^2 = 2\sum H_\iota \omega_\iota \tag{2}$$

setzt, wo nun $H_1, H_2 \ldots H_n$ bestimmte, *mit rationalen Coefficienten* behaftete, ganze homogene quadratische Functionen der Coordinaten bedeuten. Durch diese n Functionen H_ι, auf deren analytische Eigenschaften wir unten zurückkommen werden, ist die Constitution des Körpers Ω vollständig bestimmt, und es lässt sich zunächst zeigen, dass die Zahlen von der Form (1) auch durch Division sich wieder erzeugen. Durch totale Differentiation von (2) erhält man

$$\omega\, d\omega = \sum dH_\iota \omega_\iota; \tag{3}$$

legt man den Coordinaten h_ι und ihren Differentialen dh_ι beliebige rationale Werthe bei, so ist durch die vorstehende Gleichung das Product aus zwei beliebigen Zahlen ω und $d\omega$ des Körpers Ω auf die Form (1) zurückgeführt. Speciell ergiebt sich aus (3)

$$\omega\omega_r = \sum \frac{\partial H_\iota}{\partial h_r}\omega_\iota; \tag{4}$$

legt man nun den Coordinaten h_ι beliebige rationale Werthe bei, welche aber nicht sämmtlich verschwinden, so kann auch der entsprechende Werth der Functional-Determinante

$$H = \sum \pm \frac{\partial H_1}{\partial h_1}\frac{\partial H_2}{\partial h_2}\cdots\frac{\partial H_n}{\partial h_n} \tag{5}$$

nicht verschwinden; denn sonst liessen sich bekanntlich n rationale Zahlen dh_ι, die nicht sämmtlich verschwinden, so bestimmen, dass für jeden Index r

$$dH_r = \sum \frac{\partial H_r}{\partial h_\iota} dh_\iota = 0,$$

und folglich auch $\omega\, d\omega = 0$ würde, während doch keine der beiden Zahlen ω und $d\omega$ verschwindet. Hieraus folgt weiter durch Umkehrung der n Gleichungen (4), dass die n Quotienten $\omega_\iota : \omega$ wieder Zahlen von der Form (1) sind; dasselbe gilt daher auch von jedem Quotienten $\alpha : \omega$, wo α irgend eine Zahl von der Form (1) bedeutet. Mithin bilden alle Zahlen von der Form (1) wirklich einen Körper.

Durch Elimination der n Zahlen ω_ι aus den n Gleichungen (4) ergiebt sich die Gleichung

$$\begin{vmatrix} \frac{\partial H_1}{\partial h_1} - \omega, & \frac{\partial H_2}{\partial h_1} & \cdots & \frac{\partial H_n}{\partial h_1} \\ \frac{\partial H_1}{\partial h_2}, & \frac{\partial H_2}{\partial h_2} - \omega & \cdots & \frac{\partial H_n}{\partial h_2} \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots & & & \\ \frac{\partial H_1}{\partial h_n}, & \frac{\partial H_2}{\partial h_n} & \cdots & \frac{\partial H_n}{\partial h_n} - \omega \end{vmatrix} = 0 \qquad (6)$$

mithin ist jede Zahl ω des Körpers Ω die Wurzel einer (von der Wahl der Basis unabhängigen) Gleichung $n$ten Grades mit rationalen Coefficienten, also eine *algebraische Zahl*, und es lässt sich leicht zeigen, dass in dem Körper Ω auch Zahlen existiren, welche keiner Gleichung mit rationalen Coefficienten von niedrigerem als dem $n$ten Grade genügen, für welche also die vorstehende Gleichung *irreductibel* ist*). Bedeutet θ eine solche Zahl, so bilden

---

*) Der Beweis dieser Behauptung kann z. B. auf das folgende Lemma gestützt werden:

Genügt eine homogene lineare Function $\omega = \Sigma h_\iota \omega_\iota$ der n Variabeln h_ι einer Identität von der Form

$$A\omega^m + A_1\omega^{m-1} + \cdots + A_m = 0, \qquad (1)$$

wo A, $A_1 \ldots A_m$ ganze Functionen der Variabeln h_ι mit *rationalen* Coefficienten bedeuten, die nicht sämmtlich identisch verschwinden, und ist der Grad m *kleiner* als die Anzahl n der Variabeln, so sind die n Grössen ω_ι von einander *abhängig*.

Durch totale Differentiation der Identität (1) ergiebt sich zunächst

$$M d\omega + \omega^m dA + \omega^{m-1} dA_1 + \cdots + dA_m = 0, \qquad (2)$$

wo zur Abkürzung

$$M = mA\omega^{m-1} + (m-1)A_1\omega^{m-2} + \cdots + A_{m-1}$$

gesetzt ist. Man kann nun offenbar annehmen, dass keine solche Identität (1) von noch niedrigerm Grade als m existirt, dass also das Product AM nicht identisch verschwindet; nun lege man, was stets möglich ist, den Variabeln h_ι solche rationale Werthe bei, für welche AM einen von Null verschiedenen Werth erhält; hierauf kann man, weil $m < n$ ist, den n Differentialen dh_ι solche rationale Werthe beilegen, welche den m homogenen linearen Gleichungen

$$AdA_1 = A_1 dA,\ AdA_2 = A_2 dA \ldots AdA_m = A_m dA$$

genügen und nicht sämmtlich verschwinden; multiplicirt man nun (1) mit dA, (2) mit A, und subtrahirt, so folgt $AMd\omega = 0$, also auch $d\omega = \Sigma dh_\iota \omega_\iota = 0$, was zu beweisen war.

Hieraus folgt zunächst, dass, wenn die Grössen ω_ι und ω wieder ihre alte Bedeutung erhalten, die aus den Coordinaten der n Grössen 1, ω, $\omega^2 \ldots \omega^{n-1}$ gebildete Determinante D, welche eine homogene Function der

offenbar die Potenzen $1, \theta, \theta^2 \ldots \theta^{n-1}$ ebenfalls eine Basis des Körpers Ω, und Ω ist das System aller Zahlen, welche sich durch beliebige Wiederholung der vier arithmetischen Grundoperationen aus θ ableiten lassen. Substituirt man nun für θ der Reihe nach alle Wurzeln derselben irreductibelen Gleichung, so entstehen ebensoviele entsprechende Körper welche offenbar mit Ω und folglich auch mit einander conjugirt sind, und es liesse sich leicht zeigen, dass ausser diesen Körpern kein anderer mit Ω conjugirt ist. Dabei bemerken wir aber, um Missverständnissen vorzubeugen, dass diese n Körper, was ihren gesammten Zahleninhalt anbetrifft, sehr wohl theilweise oder auch sämmtlich identisch sein können, obgleich sie durch n *verschiedene* Substitutionen aus einem von ihnen hervorgehen *).

Da nun vermöge des Begriffes conjugirter Körper die Gleichungen (4) gültig bleiben, wenn die Zahlen des Körpers Ω durch die entsprechenden Zahlen eines conjugirten Körpers ersetzt werden, so folgt leicht, dass die sämmtlichen Wurzeln der Gleichung (6) die mit ω conjugirten Zahlen sind. Bezeichnet man daher mit $N(\omega)$ die sogenannte *Norm* der Zahl ω, d. h. das Product aus allen n conjugirten Wurzeln, die auch gruppenweise einander gleich sein können, so ist zufolge (6)

$$N(\omega) = H, \tag{7}$$

d. h. die homogene Function H ist das Product aus n conjugirten Factoren ersten Grades mit algebraischen Coefficienten. Aus dieser

---

Variabeln h_t vom Grade $\frac{1}{2}n(n-1)$ ist, nicht identisch verschwinden kann, weil sonst ω einer Identität von der obigen Form (1) und von niedrigerem Grade als n genügte, und folglich die Grössen ω_t von einander abhängig wären. Giebt man nun den Coordinaten h_t solche rationale Werthe, für welche D einen von Null verschiedenen Werth erhält, so folgt unmittelbar, dass die entsprechende Zahl ω des Körpers Ω die Wurzel einer irreductibeln Gleichung $n$ten Grades ist.

Jeder Lösung der Gleichung $D = 0$ in rationalen Zahlen h_t entspricht eine Zahl ω, welche einem Divisor des Körpers Ω von niedrigerem als dem $n$ten Grade angehört; der Grad eines solchen Divisors ist immer ein Divisor von n.

*) Durch die weitere Verfolgung dieses Gegenstandes gelangt man unmittelbar zu den von *Galois* in die Algebra eingeführten Principien (*Sur les conditions de résolubilité des équations par radicaux*; Journ. de Math. p. p. Liouville. T. XI. 1846); hierbei ist es zweckmässig, zunächst die einfachen Reciprocitätsgesetze aufzusuchen, welche zwischen irgend zwei solchen Körpern wie Ω, ihrem grössten gemeinschaftlichen Divisor und ihrem kleinsten gemeinschaftlichen Multiplum herrschen.

Definition geht unmittelbar der Satz hervor: *die Norm eines Productes ist immer gleich dem Product aus den Normen der Factoren.* Setzt man ferner

$$N(\omega) = \omega\,\omega', \tag{8}$$

so ist ω', weil $N(\omega)$ als rationale Zahl in Ω enthalten ist, ebenfalls eine Zahl des Körpers Ω, was auch aus (6) hervorgeht, und zwar ist

$$N(\omega') = N(\omega)^{n-1}; \tag{9}$$

nennen wir ω' die *zu* ω *adjungirte Zahl**), so ist die zu ω' adjungirte Zahl $= \omega\,N(\omega)^{n-2}$.

Sind $\alpha_1, \alpha_2 \ldots \alpha_n$ beliebige Zahlen des Körpers Ω, und bedeuten $\beta_\iota, \gamma_\iota \ldots \lambda_\iota$ die übrigen $(n-1)$ mit α_ι conjugirten Zahlen, so setzen wir zur Abkürzung

$$(\Sigma \pm \alpha_1\beta_2 \ldots \lambda_n)^2 = \Delta(\alpha_1, \alpha_2 \ldots \alpha_n) \tag{10}$$

und nennen dieses Determinantenquadrat die *Discriminante* der n Zahlen $\alpha_1, \alpha_2 \ldots \alpha_n$; sie ist eine symmetrische Function der n mit θ conjugirten Zahlen und folglich eine *rationale* Zahl, und zwar ist

$$\Delta(\alpha_1, \alpha_2 \ldots \alpha_n) = m^2\,\Delta(\omega_1, \omega_2 \ldots \omega_n), \tag{11}$$

wo m die aus den Coordinaten der Zahlen $\alpha_1, \alpha_2 \ldots \alpha_n$ gebildete Determinante bedeutet; da die Discriminante $\Delta(1, \theta, \theta^2 \ldots \theta^{n-1})$ bekanntlich das Product aller Differenzen zwischen den mit θ conjugirten Zahlen und folglich von Null verschieden ist (weil eine irreductibele Gleichung nur ungleiche Wurzeln haben kann), so ist $\Delta(\alpha_1 \ldots \alpha_n)$ stets und nur dann $=0$, wenn die Zahlen $\alpha_1, \alpha_2 \ldots \alpha_n$ von einander abhängig sind. Endlich ist allgemein

$$\Delta(\omega\alpha_1, \omega\alpha_2 \ldots \omega\alpha_n) = N(\omega)^2\,\Delta(\alpha_1, \alpha_2 \ldots \alpha_n). \tag{12}$$

II. Im Vorhergehenden sind die Begriffe und Sätze entwickelt, deren wir in der Folge bedürfen; zur Erläuterung mögen aber hier noch die wichtigsten und nächstliegenden Resultate aus dem grossen Reichthume analytischer Entwicklungen mitgetheilt werden, welche sich an die Betrachtung der Functionen H_ι anknüpfen. Zwischen diesen n Functionen bestehen fundamentale Relationen, welche man erhält, wenn man das Product aus *drei* beliebigen Zahlen des Körpers Ω auf alle möglichen Arten bildet (vergl. §§. 1, 2). Bedeutet d' wieder eine beliebige Variation, so ist zufolge (4)

---

*) Dieser Ausdruck wird hier in ganz anderer Bedeutung gebraucht, wie von *Galois*.

$$d'\omega\,\omega_r = \Sigma\, d'\left(\frac{\partial H_\iota}{\partial h_r}\right)\omega_\iota;$$

multiplicirt man nun (3) mit $d'\omega$, und ersetzt die Producte $d'\omega\,\omega_\iota$ der vorstehenden Gleichung gemäss durch Summen, so folgt

$$\omega\, d\omega\, d'\omega = \Sigma\, dH_\iota d'\left(\frac{\partial H_{\iota'}}{\partial h_\iota}\right)\omega_{\iota'};$$

da die linke Seite symmetrisch in Bezug auf d und d' ist, und da die n Zahlen $\omega_{\iota'}$ unabhängig sind, so ergiebt sich, dass die Functionen H_ι den n Differentialgleichungen

$$\Sigma\, dH_\iota d'\left(\frac{\partial H_r}{\partial h_\iota}\right) = \Sigma\, d'H_\iota d\left(\frac{\partial H_r}{\partial h_\iota}\right) \tag{13}$$

genügen, wo r irgend einen der Indices $1, 2 \ldots n$ bedeutet. Um die Bedeutung dieser Relationen mehr hervortreten zu lassen, wollen wir sie den folgenden Entwicklungen zu Grunde legen, ohne den Zusammenhang der Functionen H_ι mit dem Körper Ω zu benutzen.

Zunächst wollen wir zeigen, dass die Functionaldeterminante H, welche zufolge ihrer Definition (5) eine ganze homogene Function $n$ten Grades mit rationalen Coefficienten ist, sich durch Multiplication reproducirt; gehen die Formen K und L dadurch aus H hervor, dass die Coordinaten h_ι resp. durch dh_ι und durch dH_ι ersetzt werden, so ist

$$L = HK; \tag{14}$$

denn wenn man die Coordinaten h_ι durch dh_ι ersetzt, so geht jede homogene lineare Function

$$\frac{\partial H_r}{\partial H_s} \quad \text{in} \quad d\left(\frac{\partial H_r}{\partial h_s}\right),$$

und folglich H in

$$K = \Sigma \pm d\left(\frac{\partial H_1}{\partial h_1}\right) d\left(\frac{\partial H_2}{\partial h_2}\right) \cdots d\left(\frac{\partial H_n}{\partial h_n}\right)$$

über; werden aber die Coordinaten h_ι durch die bilinearen Functionen dH_ι ersetzt, so geht zufolge (13)

$$\frac{\partial H_r}{\partial h_s} \quad \text{in} \quad \Sigma\, \frac{\partial}{\partial h_s}\left(\frac{\partial H_r}{\partial h_\iota}\right) dH_\iota = \Sigma\, \frac{\partial H_\iota}{\partial h_s}\, d\left(\frac{\partial H_r}{\partial h_\iota}\right),$$

und folglich H in $L = HK$ über, was zu beweisen war. Dies ist der schon oben angeführte Satz über die Norm eines Productes.

Bedeutet φ eine willkürliche Function der Coordinaten h_t, und definirt man die Variation δ dadurch, dass

$$\delta\varphi = \Sigma \frac{\partial \varphi}{\partial H_t} h_t, \quad \text{also} \quad \delta H_t = h_t \tag{15}$$

wird, so ergiebt sich aus (13), wenn man d' durch δ ersetzt,

$$\Sigma\, dH_t \delta\left(\frac{\partial H_r}{\partial h_t}\right) = \Sigma h_t d\left(\frac{\partial H_r}{\partial h_t}\right) = dH_r,$$

weil H_r eine homogene Function zweiten Grades ist, mithin

$$\delta\left(\frac{\partial H_r}{\partial h_s}\right) = 1 \quad \text{oder} \quad = 0 \tag{16}$$

je nachdem r und s gleich oder ungleich sind; hieraus folgt, dass die n Variationen δh_t *constante, rationale Zahlen* sind. Wird ferner die Variation δ' durch

$$\delta'\varphi = H \Sigma \frac{\partial \varphi}{\partial H_t} \delta h_t, \quad \text{also} \quad \delta' H_t = H \delta h_t \tag{17}$$

definirt, so ergiebt sich, wenn man in (13) d' durch δ' ersetzt,

$$\Sigma\, dH_t \delta'\left(\frac{\partial H_r}{\partial h_t}\right) = H \Sigma \delta h_t d\left(\frac{\partial H_r}{\partial h_t}\right) = Hd \Sigma \frac{\partial H_r}{\partial h_t} \delta h_t$$
$$= Hd\delta H_r = Hdh_r,$$

folglich

$$\delta'\left(\frac{\partial H_r}{\partial h_s}\right) = H \frac{\partial h_r}{\partial H_s}; \tag{18}$$

da nun der Ausdruck rechter Hand der Coefficient des Elementes

$$\frac{\partial H_s}{\partial h_r}$$

in der Determinante H, also eine *ganze homogene Function* $(n-1)$*ten Grades* der Coordinaten h_t mit rationalen Coefficienten ist, so gilt dasselbe von den Grössen

$$h'_r = \delta' h_r = H \Sigma \frac{\partial h_r}{\partial H_t} \delta h_t, \tag{19}$$

und umgekehrt geht aus (18) hervor, dass die Coefficienten der einzelnen n^2 Elemente in der Determinante H sich als homogene lineare Functionen der soeben definirten n Grössen h'_t darstellen lassen. Wir wollen, wenn φ eine beliebige Function der Coordinaten h_t bedeutet, mit φ' dieselbe Function der Grössen h'_t bezeichnen; dann lautet die Gleichung (18)

$$\frac{\partial H'_r}{\partial h'_s} = H \frac{\partial h_r}{\partial H_s}, \tag{20}$$

und hieraus folgt zugleich

$$H' = H^{n-1}; \quad H \frac{\partial h'_s}{\partial H'_r} = \frac{\partial H_s}{\partial h_r}. \tag{21}$$

Da H eine Functionaldeterminante ist, so ist bekanntlich*)

$$d \log H = \Sigma \frac{\partial d H_t}{\partial H_t} - \Sigma \frac{\partial d h_t}{\partial h_t},$$

und folglich ergiebt sich unter Berücksichtigung von (13)

$$\Sigma \frac{\partial \log H}{\partial h_t} d H_t = \Sigma \frac{\partial}{\partial H_{t'}} \left(\frac{\partial H_{t'}}{\partial h_t} \right) d H_t$$

$$= \Sigma d \left(\frac{\partial H_{t'}}{\partial h_t} \right) \frac{\partial H_t}{\partial H_{t'}} = d \Sigma \frac{\partial H_t}{\partial h_t};$$

führt man daher die *homogene lineare Function*

$$S = \Sigma \frac{\partial H_t}{\partial h_t} \tag{22}$$

ein, so ist

$$\Sigma \frac{\partial \log H}{\partial h_t} d H_t = d S; \quad \frac{\partial \log H}{\partial h_r} = \frac{\partial S}{\partial H_r}, \tag{23}$$

also mit Rücksicht auf (20)

$$\frac{\partial H}{\partial h_r} = H \Sigma \frac{\partial S}{\partial h_t} \frac{\partial h_t}{\partial H_r} = \Sigma \frac{\partial S}{\partial h_t} \frac{\partial H'_t}{\partial h'_r};$$

man führe daher die *ganze homogene Function zweiten Grades*

$$T = \Sigma \frac{\partial S}{\partial h_t} H_t \tag{24}$$

ein, so wird

$$\frac{\partial H}{\partial h_r} = \frac{\partial T}{\partial h'_r}; \quad d H = \Sigma \frac{\partial T}{\partial h'_t} d h_t, \tag{25}$$

mithin sind auch die Derivirten der Form H darstellbar als homogene lineare Functionen der in (19) definirten Grössen h'_t, und rückwärts diese durch jene. Da ferner zufolge (20)

*) *Jacobi: De determinantibus functionalibus* §. 9 (Crelle's Journal XXII); in der obigen Form ist auch der Fall berücksichtigt, dass die Differentiale $d h_t$ Functionen von den Veränderlichen h_t sind. Ersetzt man d durch δ', so folgt aus (17) und (19) unmittelbar

$$\Sigma \frac{\partial h'_t}{\partial h_t} = 0.$$

$$\Sigma \frac{\partial H_t'}{\partial h_s'} \frac{\partial H_r}{\partial h_t} = H \text{ oder } = 0$$

ist, je nachdem r und s gleich oder ungleich sind, so folgt durch Multiplication mit h_s' oder dh_s' und Summation in Bezug auf s

$$2 \Sigma H_t' \frac{\partial H_r}{\partial h_t} = Hh_r'; \quad \Sigma dH_t' \frac{\partial H_r}{\partial h_t} = Hdh_r'$$

und hieraus durch Differentiation

$$h_r' dH - Hdh_r' = 2 \Sigma H_t' d\left(\frac{\partial H_r}{\partial h_t}\right). \tag{26}$$

Mit Hülfe von (25) und (26) ist man im Stande, auch die Differentiale höherer Ordnung von H zu bilden; auf diese Weise findet man

$$Hdd'H - dHd'H = 2H \Sigma \frac{\partial H}{\partial h_t} dd'h_t - 2 \Sigma \frac{\partial^2 T}{\partial h_t \partial h_{t'}} H_t' dd' H_{t'}; \tag{27}$$

ausserdem ergiebt sich aus Gleichung (26), welcher man mit Hülfe von (13) auch die Form

$$h_r' dH - Hdh_r' = \Sigma \frac{\partial H_t'}{\partial h_{t'}'} \frac{\partial H_r'}{\partial h_t'} dh_{t'}$$

geben kann, die Functionaldeterminante

$$\Sigma \pm \frac{\partial h_1'}{\partial h_1} \frac{\partial h_2'}{\partial h_2} \cdots \frac{\partial h_n'}{\partial h_n} = (-1)^{n-1}(n-1) H^{n-2} \tag{28}$$

und folglich aus (25) die Hesse'sche Determinante der Form H, nämlich

$$\Sigma \pm \frac{\partial^2 H}{\partial h_1^2} \cdots \frac{\partial^2 H}{\partial h_n^2} = (-1)^{n-1}(n-1) H^{n-2} \Sigma \pm \frac{\partial^2 T}{\partial h_1^2} \cdots \frac{\partial^2 T}{\partial h_n^2}. \tag{29}$$

Aus den Gleichungen (16), (22), (24), (25), (26), (27) ergeben sich unmittelbar folgende auf die Variation δ bezüglichen Resultate:

$$\begin{aligned} &\delta S = n; \quad \delta T = S; \quad h_r' \delta H - H \delta h_r' = 2 H_r'; \\ &\delta H = S'; \quad \delta' H = \delta H^2 - H \delta^2 H = 2 T'. \end{aligned} \tag{30}$$

III. Alle diese Sätze sind abgeleitet aus der Voraussetzung, dass das System der n ganzen homogenen Functionen H_t vom zweiten Grade den Bedingungen (13) genügt, und dass ihre Functionaldeterminante H nicht identisch verschwindet; fügt man noch die Voraussetzung hinzu, dass die Coefficienten dieser Functionen

rationale Zahlen sind, und dass die Form H *irreductibel*, d. h. nicht zerlegbar ist in Factoren niedrigeren Grades, deren Coefficienten ebenfalls rationale Zahlen sind, so lässt sich umgekehrt beweisen, dass zu diesem Functionensystem ein algebraischer Zahlkörper Ω von der oben betrachteten Art gehört. Der Kürze halber führen wir eine Charakteristik ε ein, welche folgenden Sinn hat: ist φ irgend eine Function der Coordinaten h_ι, und ersetzt man die letzteren durch $h_\iota - \omega \delta h_\iota$, wo ω vorläufig eine *willkürliche* Function bedeutet, so geht φ in eine neue Function über, welche mit $\varepsilon(\varphi)$ bezeichnet werden soll. Aus dieser Definition folgt sofort

$$d\,\varepsilon(\varphi) = \varepsilon(d\varphi) - \varepsilon(\delta\varphi)\,d\omega; \tag{31}$$

unter der Voraussetzung, dass die Differentiale dh_ι *constant* sind. Hierauf definire man die Function ω als Wurzel der Gleichung $n$ten Grades

$$\varepsilon(H) = 0, \tag{32}$$

welche zufolge (16) vollständig mit der Gleichung (6) übereinstimmt, so lässt sich beweisen, dass ω eine *ganze* (homogene) Function ersten Grades, d. h. dass $dd'\omega = 0$ ist, wenn die Differentiale dh_ι, $d'h_\iota$ als constant vorausgesetzt werden. In der That ergiebt sich durch successive Differentiation der Identität (32) nach der in (31) ausgesprochenen Regel

$$\varepsilon(\delta H)\,d\omega = \varepsilon(dH) \tag{33}$$

und

$$\varepsilon(\delta H)^3\,d\,d'\omega = \varepsilon(R), \tag{34}$$

wo zur Abkürzung die homogene Function $(3n-4)$ten Grades

$$\left\{\begin{array}{c} \delta H^2 d d' H + \delta^2 H d H d' H \\ -\delta H d H d' \delta H - \delta H d' H d \delta H \end{array}\right\} = R$$

gesetzt ist. Dass diese Function R durch H theilbar, in Zeichen, dass $R \equiv 0$ ist*), ergiebt sich auf folgende Weise.

Aus (30) folgt

$$h'_r \delta H = 2H'_r + H\delta h'_r \equiv 2H'_r$$

ferner

$$h'_r \delta^2 H = 2\,\delta H'_r + H\delta^2 h'_r \equiv 2\,\delta H'_r$$

und hieraus durch Elimination von h'_r

$$\delta^2 H H'_r - \delta H \delta H'_r \equiv 0;$$

*) Dies gilt allgemein von dem Ausdrucke

$$d'H\,d'''H\,dd''H + dH\,d''H\,d'd'''H - d'''H\,dH\,d'd''H - d'H\,d''H\,dd'''H.$$

da nun zufolge (27) $dHd'H - Hdd'H$ eine homogene lineare Function der n Grössen H_i' ist, so folgt auch, dass

$$\delta^2 H(dHd'H - Hdd'H) - \delta H\delta(dHd'H - Hdd'H) \equiv 0$$

ist; die linke Seite unterscheidet sich aber von R nur um Bestandtheile, welche durch H theilbar sind. Mithin ist $R = PH$, wo P eine ganze Function bedeutet, und folglich $\varepsilon(R) = \varepsilon(P)\varepsilon(H) = 0$. Da sich nun aus den Voraussetzungen über H beweisen lässt, dass $\varepsilon(\delta H)$ nicht identisch verschwindet, so folgt aus (34) $dd'\omega = 0$, d. h. die Wurzel ω der Gleichung (32) ist eine ganze Function ersten Grades; dass sie zugleich homogen ist, versteht sich von selbst, weil H, $\delta H \ldots \delta^{n-1}H$ und folglich auch ω gleichzeitig mit den Coordinaten h_i verschwinden. Setzt man nun

$$\frac{\partial\omega}{\partial h_i} = \omega_i, \quad \omega = \Sigma h_i\omega_i, \tag{1}$$

so ergiebt sich aus (33), dass

$$\Sigma \delta h_i \omega_i = \delta\omega = 1 \tag{35}$$

und

$$\varepsilon\left(\frac{\partial H}{\partial h_i}\right) = \varepsilon(\delta H)\,\omega_i \tag{36}$$

ist. Da ferner zufolge (23)

$$\Sigma \frac{\partial H}{\partial h_i} dH_i = HdS \equiv 0$$

und

$$\varepsilon(dH_i) = dH_i - \omega d\delta H_i = dH_i - \omega dh_i$$

ist, so folgt

$$0 = \varepsilon(H)dS = \Sigma\, \varepsilon\left(\frac{\partial H}{\partial h_i}\right)\varepsilon(dH_i)$$
$$= \varepsilon(\delta H)\, \Sigma\, \omega_i(dH_i - \omega dh_i),$$

mithin

$$\omega d\omega = \Sigma\, dH_i\omega_i, \tag{3}$$

also auch

$$\omega^2 = 2\Sigma H_i\omega_i, \tag{2}$$

wodurch wir rückwärts zu unseren ursprünglichen Annahmen zurückgekehrt sind; und man kann auch beweisen — worauf wir hier nicht eingehen wollen — dass aus den Voraussetzungen über H die *Unabhängigkeit* der n Zahlen ω_i folgt.

Wir fügen diesen Entwicklungen endlich noch folgende leicht zu beweisende Bemerkungen hinzu. Die ausgeführte Form der Gleichung (32) oder (6) ist folgende

$$0 = H - \delta H \frac{\omega}{1} + \delta^2 H \frac{\omega^2}{1.2} - \delta^3 H \frac{\omega^3}{1.2.3} + \cdots; \quad (37)$$

es ist ferner

$$H = \Pi \omega = N(\omega), \quad (7)$$

wo das Productzeichen Π sich auf alle n Wurzeln ω bezieht; ebenso findet man (wenn man in (3) d durch δ' ersetzt)

$$H = \omega \omega', \quad (8)$$

wo

$$\omega' = \delta' \omega = \Sigma h_i' \omega_i \quad (38)$$

zu ω adjungirt ist, und

$$S = \Sigma \omega, \quad 2T = \Sigma \omega^2, \quad (39)$$

wo die Summenzeichen sich ebenfalls auf alle n Wurzeln beziehen. Die quadratische Form T ist charakteristisch für die Anzahl der reellen Wurzeln; bildet man ferner die Hesse'sche Determinante des Productes $H = \Pi \omega$, so ergiebt sich durch Vergleichung mit (29) die Discriminante

$$\Delta(\omega_1, \omega_2 \ldots \omega_n) = \Sigma \pm \frac{\partial^2 T}{\partial h_1^2} \cdots \frac{\partial^2 T}{\partial h_n^2}, \quad (40)$$

was auch umittelbar aus (39) folgt.

§. 160.

Der Inbegriff *aller* algebraischen Zahlen bildet offenbar ebenfalls einen Körper*). Wir wollen nun, indem wir unserem eigent-

*) Dass es ausser den algebraischen noch andere, sogenannte ***transcendente*** Zahlen giebt, ist meines Wissens zuerst von *Liouville* bewiesen (***Sur des classes très-étendues de quantités dont la valeur n'est ni algébrique, ni même réductible à des irrationnelles algébriques***; Journ. de Math. T. XVI. 1851). Man vermuthet, dass die Ludolph'sche Zahl π eine solche transcendente Zahl ist; allein selbst die als specieller Fall hierin enthaltene Behauptung, dass die Quadratur des Zirkels unmöglich sei, ist bis auf den heutigen Tag noch nicht erwiesen. (Vergl. ***Euler: De relatione inter ternas pluresve quantitates instituenda.*** §. 10. Opusc. anal. T. II. 1785.)

lichen Gegenstande näher treten, eine Zahl α eine *ganze algebraische Zahl* nennen, wenn sie die Wurzel einer Gleichung ist, deren Coefficienten rationale ganze Zahlen sind, wobei wir ein- für allemal bemerken, dass wir unter den *Coefficienten* einer Function $m$ten Grades

$$F(x) = cx^m + c_1 x^{m-1} + c_2 x^{m-2} + \cdots + c_m$$

oder der Gleichung $F(x) = 0$ stets die m Quotienten

$$-\frac{c_1}{c}, \quad +\frac{c_2}{c} \cdots (-1)^m \frac{c_m}{c}$$

verstehen. Aus dieser Erklärung folgt zunächst, dass eine rationale Zahl stets und nur dann eine ganze algebraische Zahl ist, wenn sie eine ganze Zahl im gewöhnlichen Sinne des Wortes ist (vergl. §. 5, 4.); diese Zahlen wollen wir von jetzt ab *rationale ganze Zahlen*, alle algebraischen ganzen Zahlen aber kurz *ganze Zahlen* nennen. Dieses vorausgeschickt, schreiten wir zum Beweise der folgenden Fundamentalsätze.

1. *Die Summe, die Differenz und das Product zweier ganzen Zahlen α, β sind wieder ganze Zahlen.*

Sind a, b resp. die Grade der Gleichungen $\varphi(\alpha) = 0$, $\psi(\beta) = 0$, deren Coefficienten rationale ganze Zahlen sind, und bezeichnet man mit $\omega_1, \omega_2 \ldots \omega_n$ die sämmtlichen ab Producte von der Form $\alpha^{a'}\beta^{b'}$, wo a' irgend eine der Zahlen $0, 1, 2 \ldots (a-1)$, und b' irgend eine der Zahlen $0, 1, 2 \ldots (b-1)$ bedeutet, so wird, wenn $\omega = \alpha + \beta$, oder $= \alpha - \beta$, oder $= \alpha\beta$ ist, jedes der n Producte $\omega\omega_1$, $\omega\omega_2 \ldots \omega\omega_n$ mit Zuziehung der Gleichungen $\varphi(\alpha) = 0$, $\psi(\beta) = 0$ auf die Form $r_1\omega_1 + r_2\omega_2 + \cdots + r_n\omega_n$ gebracht werden können, wo $r_1, r_2 \ldots r_n$ rationale ganze Zahlen sind. Eliminirt man die n Grössen $\omega_1, \omega_2 \ldots \omega_n$ aus diesen n Gleichungen, so ergiebt sich für ω eine Gleichung vom $n$ten Grade (wie (6) in §. 159), deren Coefficienten rationale ganze Zahlen sind, was zu beweisen war (vergl. §. 139).

2. Die ganze Zahl α heisst *theilbar* durch die ganze Zahl β, oder ein *Multiplum* von β, wenn der Quotient $\alpha : \beta$ ebenfalls eine ganze Zahl ist; umgekehrt heisst β ein *Divisor* oder *Theiler* von α (vergl. §. 3). Ebenso setzen wir $\alpha \equiv \beta \pmod{\gamma}$, wenn $\alpha - \beta$ durch γ theilbar ist, und nennen α, β *congruent nach dem Modul γ* (vergl. §. 17). Man erkennt sofort (zufolge 1.), dass die Sätze des §. 3 und auch die des §. 17 (mit *vorläufiger* Ausnahme von 6. und 8.; vergl. §. 164, 3.) ihre Gültigkeit behalten.

3. *Jede Wurzel ω einer Gleichung, deren Coefficienten ganze Zahlen sind, ist ebenfalls eine ganze Zahl.*

Ist ω die Wurzel einer Gleichung $m$ten Grades $F(\omega) = 0$, deren Coefficienten $\alpha, \beta \ldots$ ganze Zahlen sind, sind ferner $a, b \ldots$ resp. die Grade der mit rationalen ganzen Coefficienten behafteten Gleichungen $\varphi(\alpha) = 0$, $\psi(\beta) = 0 \ldots$, so führe man die sämmtlichen $m\,a\,b \ldots$ Producte $\omega_1, \omega_2 \ldots \omega_n$ von der Form $\omega^{m'} \alpha^{a'} \beta^{b'} \ldots$ ein, wo die ganzen rationalen Exponenten den Bedingungen $0 \leqq m' < m$, $0 \leqq a' < a$, $0 \leqq b' < b \ldots$ genügen; dann lässt sich vermöge der Gleichungen $F(\omega) = 0$, $\varphi(\alpha) = 0$, $\psi(\beta) = 0 \ldots$ jedes der n Producte $\omega\omega_1$, $\omega\omega_2 \ldots \omega\omega_n$ wieder in die Form $r_1\omega_1 + r_2\omega_2 + \cdots + r_n\omega_n$ bringen, wo $r_1, r_2 \ldots r_n$ rationale ganze Zahlen bedeuten, und hieraus folgt unmittelbar die Richtigkeit des Satzes.

Ist daher z. B. α eine ganze Zahl, und r eine beliebige (ganze oder gebrochene) *positive* rationale Zahl, so ist auch α^r eine ganze Zahl (vergl. §. 5, 4.).

4. Bekanntlich lassen sich die Begriffe der Theilbarkeit und des Vielfachen von den ganzen rationalen Zahlen unmittelbar auf die ganzen rationalen Functionen übertragen, und es giebt einen Algorithmus zur Auffindung des grössten gemeinschaftlichen Divisors $\varphi(x)$ zweier gegebenen Functionen $F(x), f(x)$, welcher demjenigen der Zahlentheorie (§. 4) vollständig analog ist. Sind die Coefficienten von $F(x)$ und $f(x)$ sämmtlich in einem Körper K enthalten, so werden auch die Coefficienten von $\varphi(x)$ Zahlen des Körpers K sein, weil sie durch Addition, Multiplication, Subtraction und Division aus den Coefficienten von $F(x)$ und $f(x)$ entstehen. Hieraus folgt leicht, dass, wenn α die Wurzel einer solchen Gleichung $F(\alpha) = 0$ ist, deren Coefficienten Zahlen des Körpers K sind, nothwendig auch eine solche Gleichung $\varphi(\alpha) = 0$ von *niedrigstem Grade* existiren muss, welche *irreductibel in K* heissen soll und welche offenbar keine anderen Wurzeln besitzen kann als die Gleichung $F(\alpha) = 0$. Hieraus folgt der Satz:

Ist α eine ganze Zahl, und K ein bestimmter Körper, so sind alle Coefficienten der in K irreductibelen Gleichung $\varphi(\alpha) = 0$ ganze Zahlen.

Denn weil α eine ganze Zahl, also die Wurzel einer Gleichung $F(\alpha) = 0$ ist, deren Coefficienten rationale ganze Zahlen und folg-

lich auch Zahlen des Körpers K sind (§. 159), so kann die in K irreductibele Gleichung $\varphi(\alpha) = 0$, welcher α genügt, nur ganze Zahlen zu Wurzeln haben; da aber die Coefficienten einer Gleichung durch Addition und Multiplication aus ihren Wurzeln entstehen, so sind (zufolge 1.) auch die Coefficienten der Gleichung $\varphi(\alpha) = 0$ ganze Zahlen, was zu beweisen war.

Der einfachste Fall, in welchem K der Körper der rationalen Zahlen ist, findet sich bei *Gauss**).

5. *Ist ϱ irgend eine algebraische Zahl, so giebt es immer unendlich viele (von Null verschiedene) rationale ganze Zahlen h von der Beschaffenheit, dass $h\varrho$ eine ganze Zahl wird, und zwar stimmen diese sämmtlichen Zahlen h mit den sämmtlichen rationalen Vielfachen der kleinsten unter ihnen überein.*

Da ϱ eine algebraische Zahl, also die Wurzel einer Gleichung von der Form

$$c\varrho^m + c_1\varrho^{m-1} + c_2\varrho^{m-2} + \cdots + c_m = 0$$

ist, wo $c, c_1, c_2 \ldots c_m$ rationale ganze Zahlen bedeuten, so ergiebt sich durch Multiplication mit c^{m-1}, dass $c\varrho$ eine ganze Zahl ist. Sind ferner $a\varrho$, $b\varrho$ ganze Zahlen, wo a, b rationale ganze Zahlen bedeuten, deren grösster gemeinschaftlicher Theiler $= h$ ist, so folgt leicht (aus 1. und §. 4), dass auch $h\varrho$ eine ganze Zahl ist. Hieraus ergiebt sich unmittelbar der zu beweisende Satz.

6. **Versteht man unter einer *Einheit* eine ganze Zahl ε, welche in *allen* ganzen Zahlen aufgeht, so ist zunächst erforderlich, dass sie auch in 1 aufgeht, dass also $1 = \varepsilon\varepsilon'$, und ε' eine ganze Zahl** ist; wenn nun

$$\varepsilon^m + c_1\varepsilon^{m-1} + \cdots + c_m = 0$$

die im Körper der rationalen Zahlen irreductibele Gleichung ist, welcher ε genügt, so muss (zufolge 4.) $c_m = \pm 1$ sein, weil ε' der ebenfalls irreductibelen Gleichung

$$c_m\varepsilon'^m + c_{m-1}\varepsilon'^{m-1} + \cdots + c_1\varepsilon' + 1 = 0$$

genügt; umgekehrt, ist dies der Fall, so geht ε in 1 und folglich in allen ganzen Zahlen auf, ist also eine Einheit. Die Anzahl der Einheiten ist offenbar unbegrenzt.

Ist α theilbar durch α', und sind ε, ε' irgend welche Einheiten, so ist offenbar auch $\varepsilon\alpha$ durch $\varepsilon'\alpha'$ theilbar; hinsichtlich der Theilbarkeit verhalten sich daher alle Zahlen $\varepsilon\alpha$, welche den sämmt-

*) *D. A.* art. 42.

lichen Einheiten ε entsprechen, genau wie α. Zwei ganze Zahlen, deren Quotient keine Einheit ist, wollen wir *wesentlich verschieden* nennen.

7. Will man nun den Begriff der *Primzahl* so fassen, dass sie ausser sich selbst und den Einheiten keine wesentlich verschiedene Theiler besitzt und auch selbst keine Einheit ist, so erkennt man sofort, dass gar keine solche Zahl existirt; ist nämlich α eine ganze Zahl, aber keine Einheit, so besitzt sie immer unendlich viele wesentlich verschiedene Divisoren, z. B. die Zahlen $\sqrt{\alpha}$, $\sqrt[3]{\alpha}$, $\sqrt[4]{\alpha}$ u. s. f., welche (zufolge 3.) ganze Zahlen sind.

Dagegen lässt sich der Begriff von *relativen Primzahlen* vollständig definiren, und diese Frage wird uns überhaupt auf den richtigen Weg leiten, welcher bei den ferneren Untersuchungen einzuschlagen ist. Da von einem grössten gemeinschaftlichen Theiler zweier ganzen Zahlen *vorläufig* (vergl. §. 164, 3.) nicht gesprochen werden kann, so ist es auch unmöglich, die Definition von relativen Primzahlen so zu fassen, wie sie in der Theorie der rationalen Zahlen aufgestellt wird (§. 5); aber aus dieser Definition ergaben sich mehrere Sätze, deren jeder umgekehrt das Verhalten zweier relativen Primzahlen vollständig charakterisirt, ohne die Kenntniss ihrer sämmtlichen Divisoren vorauszusetzen. Ein solcher Satz ist z. B. der folgende (§. 7): Sind a, b relative Primzahlen, so ist jede durch a und b theilbare Zahl auch durch ab theilbar. Dieser Satz lässt sich in der That umkehren: Ist jede durch a und b theilbare Zahl auch durch ab theilbar, so sind a, b relative Primzahlen. Hätten nämlich die beiden Zahlen $a = ha'$, $b = hb'$ einen gemeinschaftlichen Theiler $h > 1$, so wäre $ha'b'$ eine durch a und b, aber nicht durch ab theilbare Zahl.

Diese Betrachtung veranlasst uns, folgende für das Gebiet aller ganzen algebraischen Zahlen gültige Erklärung aufzustellen:

Zwei von Null verschiedene ganze Zahlen α, β heissen relative Primzahlen, wenn jede durch α und β theilbare Zahl auch durch $\alpha\beta$ theilbar ist.

Vor Allem bemerken wir, dass zwei relative Primzahlen im alten Sinne des Wortes, d. h. zwei rationale ganze Zahlen a, b, deren grösster gemeinschaftlicher Divisor $= 1$ ist, auch im neuen Sinne relative Primzahlen bleiben; ist nämlich eine ganze algebraische Zahl γ theilbar durch a und b, so ist der Quotient $\varrho = \gamma : ab$ eine algebraische Zahl der Art, dass $a\varrho$ und $b\varrho$ ganze Zahlen sind; mithin muss (zufolge 5.) auch ϱ eine ganze Zahl, also γ theilbar durch

ab sein, was zu beweisen war. Dass ferner umgekehrt zwei relative Primzahlen im neuen Sinne des Wortes, welche zugleich rational sind, auch relative Primzahlen im alten Sinne sind, versteht sich zufolge der der neuen Erklärung vorausgeschickten Erörterung von selbst.

Wir nennen ferner die ganzen Zahlen $\alpha, \beta, \gamma, \delta \ldots$ kurz relative Primzahlen, wenn jede von ihnen relative Primzahl zu jeder der andern ist (vergl. §. 6); ist dann eine ganze Zahl ω durch jede von ihnen theilbar, so ist sie auch durch ihr Product theilbar (vergl. §. 7), weil, wie man leicht findet, auch der folgende Satz (§. 5, 3.) seine Gültigkeit behält: Ist jede der Zahlen $\alpha', \beta', \gamma' \ldots$ relative Primzahl zu jeder der Zahlen $\alpha'', \beta'', \gamma'', \delta'' \ldots$, so sind auch die Producte $\alpha'\beta'\gamma' \ldots$ und $\alpha''\beta''\gamma''\delta'' \ldots$ relative Primzahlen und umgekehrt.

Aber wie soll man definitiv entscheiden, ob zwei gegebene ganze Zahlen α, β relative Primzahlen sind? Man könnte versuchen, folgenden Weg einzuschlagen. Da α^{-1} und β^{-1} algebraische Zahlen sind, so giebt es (zufolge 5.) immer zwei kleinste positive ganze rationale Zahlen a, b von der Art, dass $a\alpha^{-1}$ und $b\beta^{-1}$ ganze Zahlen, d. h. dass a, b resp. durch α, β theilbar werden; zeigt sich nun, dass a, b relative Primzahlen sind, so sind auch α, β gewiss relative Primzahlen. Aber man muss sich hüten zu glauben, dass auch das Umgekehrte Statt findet, dass also die *kleinsten rationalen Multipla* a, b von zwei relativen Primzahlen α, β nothwendig selbst relative Primzahlen sein müssen. So z. B. sind in der That die beiden conjugirten Zahlen $\alpha = 2 + i$ und $\beta = 2 - i$ relative Primzahlen, und doch ist $a = b = 5$. Eine wesentliche Reduction unserer Aufgabe wird aber durch den folgenden Satz bewirkt:

Wenn zwei ganze Zahlen α, β sich in einem Körper K, dem sie selbst angehören, als relative Primzahlen bewähren, d. h. wenn jede durch α und β theilbare Zahl des Körpers K auch durch $\alpha\beta$ theilbar ist; so sind α, β wirklich relative Primzahlen.

Ist nämlich ω irgend eine durch α und durch β theilbare ganze Zahl, und ist

$$\omega^m + \gamma_1 \omega^{m-1} + \gamma_2 \omega^{m-2} + \cdots + \gamma_m = 0$$

die in K irreductibele Gleichung, welcher ω genügt, so sind (zufolge 4.) die Zahlen $\gamma_1, \gamma_2 \ldots \gamma_m$ ganze Zahlen des Körpers K; da ferner

die ganzen Zahlen $\alpha' = \omega : \alpha$ und $\beta' = \omega : \beta$ resp. den in K irreductibelen Gleichungen

$$(\alpha\alpha')^m + \gamma_1(\alpha\alpha')^{m-1} + \cdots + \gamma_m = 0$$
$$(\beta\beta')^m + \gamma_1(\beta\beta')^{m-1} + \cdots + \gamma_m = 0$$

genügen, so sind (zufolge 4.) auch die Quotienten $\gamma_n : \alpha^n$ und $\gamma_n : \beta^n$ ganze Zahlen des Körpers K; da ferner nach Voraussetzung jede durch α und β theilbare Zahl des Körpers K auch durch $\alpha\beta$ theilbar ist, so ergiebt sich leicht, dass auch jede durch α^n und β^n theilbare Zahl γ_n des Körpers K durch $\alpha^n\beta^n$ theilbar, also von der Form $\alpha^n\beta^n\gamma'_n$ ist, wo γ'_n eine ganze Zahl bedeutet; setzt man nun $\omega = \alpha\beta\omega'$, so genügt ω' der Gleichung

$$\omega'^m + \gamma'_1\omega'^{m-1} + \cdots + \gamma'_m = 0,$$

deren Coefficienten ganze Zahlen sind; mithin ist ω' (zufolge 3.) eine ganze Zahl, d. h. ω ist auch theilbar durch $\alpha\beta$, was zu beweisen war.

Hieraus geht hervor, dass man, um das gegenseitige Verhalten zweier ganzen Zahlen α, β zu untersuchen, nur den kleinsten Körper K zu bilden braucht, welchem sie beide angehören; und dieser Körper ist, wie man leicht erkennt, immer von der im vorigen Paragraphen betrachteten Beschaffenheit.

§. 161.

Um den späteren Verlauf der Darstellung nicht zu unterbrechen, schalten wir hier eine sehr allgemeine Betrachtung ein, welche für die nachfolgenden, sowie für viele andere, unserem Gegenstande fremde Untersuchungen von grossem Nutzen ist.

1. Ein System $\mathfrak{a}$ von reellen oder complexen Zahlen α, deren *Summen* und *Differenzen* demselben System $\mathfrak{a}$ angehören, soll ein *Modul* heissen; wenn die Differenz zweier Zahlen ω, ω' in $\mathfrak{a}$ enthalten ist, so wollen wir sie *congruent nach* $\mathfrak{a}$ nennen und dies durch die Congruenz

$$\omega \equiv \omega' \pmod{\mathfrak{a}}$$

andeuten. Solche Congruenzen können addirt, subtrahirt und folglich auch mit beliebigen ganzen rationalen Zahlen multiplicirt werden, wie Gleichungen. Da je zwei einer dritten congruente Zahlen

auch einander congruent sind, so kann man alle existirenden Zahlen in *Classen* (mod. $\mathfrak{a}$) eintheilen, indem man je zwei congruente Zahlen in dieselbe Classe, je zwei incongruente in zwei verschiedene Classen aufnimmt.

2. Wenn alle Zahlen eines Moduls $\mathfrak{a}$ auch Zahlen eines Moduls $\mathfrak{b}$ sind, so heisse $\mathfrak{a}$ ein *Vielfaches* von $\mathfrak{b}$, und $\mathfrak{b}$ ein *Theiler* von $\mathfrak{a}$; oder wir sagen auch, $\mathfrak{b}$ gehe in $\mathfrak{a}$ auf, $\mathfrak{a}$ sei theilbar durch $\mathfrak{b}$. Aus jeder Congruenz $\omega \equiv \omega'$ (mod. $\mathfrak{a}$) folgt auch $\omega \equiv \omega'$ (mod. $\mathfrak{b}$). Offenbar *besteht* $\mathfrak{b}$ aus einer endlichen oder unendlichen Anzahl von Classen (mod. $\mathfrak{a}$).

Sind $\mathfrak{a}$, $\mathfrak{b}$ irgend zwei Moduln, so bilden alle die Zahlen, welche gleichzeitig in $\mathfrak{a}$ und in $\mathfrak{b}$ enthalten sind, das *kleinste* gemeinschaftliche Vielfache $\mathfrak{m}$ von $\mathfrak{a}$ und $\mathfrak{b}$, weil jedes gemeinschaftliche Vielfache von $\mathfrak{a}$ und $\mathfrak{b}$ auch durch den Modul $\mathfrak{m}$ theilbar ist. Durchläuft α alle Zahlen des Moduls $\mathfrak{a}$, β alle Zahlen des Moduls $\mathfrak{b}$, so bilden die Zahlen $\alpha + \beta$ den *grössten* gemeinschaftlichen Theiler von $\mathfrak{a}$ und $\mathfrak{b}$, weil jeder gemeinschaftliche Theiler von $\mathfrak{a}$ und $\mathfrak{b}$ auch in dem Modul $\mathfrak{d}$ aufgeht.

3. Sind $\omega_1, \omega_2 \ldots \omega_n$ gegebene Zahlen, so bilden alle Zahlen von der Form

$$\omega = h_1\omega_1 + h_2\omega_2 + \cdots + h_n\omega_n, \qquad (1)$$

wo $h_1, h_2 \ldots h_n$ alle ganzen rationalen Zahlen durchlaufen, einen *endlichen* Modul $\mathfrak{o}$, und wir wollen den Complex der n Zahlen $\omega_1, \omega_2 \ldots \omega_n$, mögen sie abhängig oder unabhängig von einander sein, eine *Basis* des Moduls $\mathfrak{o}$ nennen. Dann besteht folgender Satz:

Wenn alle Zahlen ω eines endlichen Moduls $\mathfrak{o}$ durch Multiplication mit rationalen, von Null verschiedenen Zahlen in Zahlen eines Moduls $\mathfrak{m}$ verwandelt werden können, so enthält $\mathfrak{o}$ nur eine endliche Anzahl incongruenter Zahlen (mod. $\mathfrak{m}$).

Da es nämlich n rationale, von Null verschiedene Zahlen $r_1, r_2 \ldots r_n$ der Art giebt, dass die Producte $r_1\omega_1, r_2\omega_2 \ldots r_n\omega_n$ in $\mathfrak{m}$ enthalten sind, so giebt es auch eine ganze rationale, von Null verschiedene Zahl s der Art, dass alle Producte $s\omega \equiv 0$ (mod. $\mathfrak{m}$) sind. Lässt man daher jede der n ganzen rationalen Zahlen $h_1, h_2 \ldots h_n$ ein vollständiges Restsystem (mod. s) durchlaufen, so entstehen s^n Zahlen ω von der Form (1), und jede Zahl des Moduls $\mathfrak{o}$ ist wenigstens einer derselben congruent (mod. $\mathfrak{m}$); mithin ist die Anzahl der in $\mathfrak{o}$ enthaltenen, nach $\mathfrak{m}$ incongruenten Zahlen *höchstens* $= s^n$, was zu beweisen war.

Allein es ist wichtig, die Anzahl dieser incongruenten Zahlen *genau* zu bestimmen. Zu diesem Zweck betrachten wir das kleinste gemeinschaftliche Vielfache $\mathfrak{a}$ der beiden Moduln $\mathfrak{o}$ und $\mathfrak{m}$; da je zwei nach $\mathfrak{m}$ congruente Zahlen ω, ω' des Modul $\mathfrak{o}$ auch nach $\mathfrak{a}$ congruent sind, und umgekehrt, so ist unsere Aufgabe die, die Anzahl der Classen (mod. $\mathfrak{a}$) zu bestimmen, aus welchen $\mathfrak{o}$ besteht. Wir suchen daher zunächst die allgemeine Form aller in $\mathfrak{a}$ enthaltenen Zahlen

$$\alpha = k_1\omega_1 + k_2\omega_2 + \cdots + k_n\omega_n \tag{2}$$

aufzustellen, wo $k_1, k_2 \ldots k_n$ jedenfalls ganze rationale Zahlen bedeuten. Ist nun r ein bestimmter Index aus der Reihe $1, 2 \ldots n$, so giebt es unter allen den Zahlen $\alpha = \theta_r$, in welchen $k_{r+1} = 0$, $k_{r+2} = 0 \ldots k_n = 0$ ist, auch solche, in denen k_r von Null verschieden ist (z. B. $s\,\omega_r$), und unter diesen sei

$$\alpha_r = a_1^{(r)}\omega_1 + a_2^{(r)}\omega_2 + \cdots + a_r^{(r)}\omega_r \tag{3}$$

eine solche, in welcher k_r den *kleinsten* positiven Werth $a_r^{(r)}$ besitzt. Dann leuchtet ein, dass der Werth von k_r in jeder Zahl θ_r durch $a_r^{(r)}$ theilbar, also von der Form $a_r^{(r)}x_r$ ist, wo x_r eine ganze rationale Zahl bedeutet, und dass folglich $\theta_r - x_r\alpha_r = \theta_{r-1}$ eine Zahl α ist, in welcher $k_r, k_{r+1} \ldots k_n$ verschwinden. Hieraus folgt sofort, dass, nachdem man für jeden Index r eine solche particuläre Zahl α_r des Moduls $\mathfrak{a}$ aufgestellt hat*), jede Zahl α gewiss in die Form

$$\alpha = x_1\alpha_1 + x_2\alpha_2 + \cdots + x_n\alpha_n \tag{4}$$

gebracht werden kann, wo $x_1, x_2 \ldots x_n$ ganze rationale Zahlen bedeuten, aus welchen die in der Form (2) vorkommenden Zahlen $k_1, k_2 \ldots k_n$ durch die Gleichungen

$$k_r = a_r^{(r)}x_r + a_r^{(r+1)}x_{r+1} + \cdots + a_r^{(n)}x_n \tag{5}$$

abgeleitet werden; und umgekehrt sind alle Zahlen α von der Form (4) in $\mathfrak{a}$ enthalten.

Ist nun eine Zahl ω von der Form (1) gegeben, sind also $h_1, h_2 \ldots h_n$ gegebene rationale ganze Zahlen, so sind *alle* Zahlen ω' des Moduls $\mathfrak{o}$, welche ihr nach $\mathfrak{m}$ congruent sind, welche also eine Classe (mod. $\mathfrak{a}$) bilden, von der Form

$$\omega' = \omega + \alpha = h_1'\omega_1 + h_2'\omega_2 + \cdots + h_n'\omega_n, \tag{6}$$

*) Das System dieser n particulären Zahlen wird ein vollständig bestimmtes, wenn man die Bedingung hinzufügt, dass $0 \leqq a_r^{(r')} < a_r^{(r)}$ sein soll, wenn $r' > r$ ist.

wo zufolge (5)

$$h'_r = h_r + a_r^{(r)} x_r + a_r^{(r+1)} x_{r+1} + \cdots + a_r^{(n)} x_n$$

ist, und hieraus folgt, dass man successive die willkürlichen rationalen ganzen Zahlen $x_n, x_{n-1} \ldots x_2, x_1$ stets und nur auf eine einzige Art so bestimmen kann, dass die n Zahlen h'_r den Bedingungen

$$0 \leqq h'_r < a_r^{(r)} \tag{7}$$

genügen. In jeder Classe existirt daher ein und nur ein *Repräsentant* ω' von der Form (6), welcher diesen Bedingungen (7) genügt; mithin ist die *Anzahl* der verschiedenen Classen (mod. $\mathfrak{a}$), aus welchen der Modul $\mathfrak{o}$ besteht, gleich dem Producte $a'_1 a''_2 \ldots a_n^{(n)}$, d. h. gleich der *Determinante* des Coefficientensystems in den n particulären Zahlen α_r von der Form (3), welche eine Basis von $\mathfrak{a}$ bilden*).

§. 162.

Wir beschränken uns von jetzt an auf die Untersuchung der ganzen Zahlen, welche in einem endlichen Körper Ω (§. 159) enthalten sind.

1. Da jede algebraische Zahl (zufolge §. 160, 5.) durch Multiplication mit einer rationalen ganzen von Null verschiedenen Zahl in eine ganze Zahl verwandelt werden kann, so dürfen wir annehmen, dass die Zahlen $\omega_1, \omega_2 \ldots \omega_n$, welche eine Basis des Körpers Ω bilden, sämmtlich *ganze* Zahlen sind, und es wird dann (zufolge §. 160, 1.) jede Zahl

$$\omega = \sum h_\iota \omega_\iota \tag{1}$$

gewiss eine ganze Zahl sein, wenn ihre Coordinaten h_ι rationale ganze Zahlen sind; aber dies lässt sich im Allgemeinen nicht umkehren, d. h. es kann ω sehr wohl eine ganze Zahl sein, auch wenn ihre Coordinaten theilweise oder sämmtlich gebrochene Zahlen

*) Die weitere Entwicklung der allgemeinen Theorie der Moduln würde uns hier zu weit führen (vergl. §. 163); wir erwähnen nur noch folgenden Satz: Sind die Basiszahlen eines endlichen Moduls von einander abhängig, so giebt es immer eine aus unabhängigen Zahlen bestehende Basis desselben Moduls. Die eleganteste Methode, die neue Basis aufzufinden, besteht in einer Verallgemeinerung der von *Gauss* angewandten Behandlung der partialen Determinanten (*D. A.* artt. 234, 236, 279).

sind. Dies ist einer der wichtigsten Puncte der Theorie und muss deshalb vor Allem aufgeklärt werden.

Wir schicken zunächst die einleuchtende Bemerkung voraus, dass die Discriminante (§. 159, (10)) eines jeden Systems von n unabhängigen ganzen Zahlen gewiss eine von Null verschiedene rationale und zwar *ganze* Zahl ist, weil sie durch Addition, Subtraction und Multiplication aus lauter ganzen Zahlen gebildet ist. Giebt es nun wirklich in Ω eine *ganze* Zahl

$$\beta = \frac{\sum k_\iota \omega_\iota}{s} \tag{2}$$

wo $s, k_1, k_2 \ldots k_n$ ganze rationale Zahlen ohne gemeinschaftlichen Theiler bedeuten, deren erste $s > 1$ ist, so behaupten wir, dass s^2 in der Discriminante $\Delta(\omega_1, \omega_2 \ldots \omega_n)$ aufgeht, und dass man eine neue Basis von ganzen Zahlen $\beta_1, \beta_2 \ldots \beta_n$ aufstellen kann, deren Discriminante absolut genommen $< \Delta(\omega_1, \omega_2 \ldots \omega_n)$ ist.

Um dies zu beweisen, bezeichnen wir mit $\mathfrak{m}$ den aus allen durch s theilbaren ganzen Zahlen bestehenden Modul, ebenso mit $\mathfrak{o}$ das System aller Zahlen ω von der Form (1), deren Coordinaten h_ι *ganze* Zahlen sind; da jedes Product $s\omega$ eine Zahl des Moduls $\mathfrak{m}$ ist, so können wir die allgemeine Untersuchung des vorigen Paragraphen auf unsern Fall anwenden. Alle durch s theilbaren Zahlen α des Systems $\mathfrak{o}$ sind daher von der Form

$$\alpha = \sum x_\iota \alpha_\iota = s \sum x_\iota \beta_\iota,$$

wo die n Zahlen $\alpha_\iota = s\beta_\iota$ particuläre Zahlen α, also die β_ι *ganze* Zahlen des Körpers Ω, und die x_ι willkürliche rationale ganze Zahlen bedeuten.

Da nun alle Zahlen $s\omega$ auch solche Zahlen α sind, so kann man

$$\omega_r = \sum b_\iota^{(r)} \beta_\iota, \quad \Delta(\omega_1, \omega_2 \ldots \omega_n) = b^2 \Delta(\beta_1, \beta_2 \ldots \beta_n)$$

setzen, wo die Coefficienten $b_\iota^{(r)}$ rationale ganze Zahlen sind, und b die aus ihnen gebildete Determinante bedeutet; durch Umkehrung ergiebt sich, dass die n Producte $b\beta_\iota$, mithin auch alle Quotienten $b\alpha : s$ *Zahlen des Systems* $\mathfrak{o}$ sind.

Wenden wir dies Resultat auf die obige Voraussetzung (2) an, dass die Zahl β eine ganze Zahl, ihr Zähler $\sum k_\iota \omega_\iota$ also eine Zahl α ist, obgleich die Zahlen $s, k_1, k_2 \ldots k_n$ keinen gemeinschaftlichen Theiler haben, so folgt unmittelbar, dass b *durch* s *theilbar* ist, wodurch zugleich die obigen Behauptungen erwiesen sind.

Da nun die Discriminante eines jeden Systems von n unabhängigen ganzen Zahlen des Körpers Ω eine von Null verschiedene ganze rationale Zahl ist, so giebt es unter allen diesen Discriminanten eine solche, deren Werth — abgesehen vom Vorzeichen — ein *Minimum* ist, und aus der vorstehenden Untersuchung folgt unmittelbar, dass, wenn eine Basis aus solchen ganzen Zahlen $\omega_1, \omega_2 \ldots \omega_n$ besteht, deren Discriminante diesen Minimumwerth besitzt, die entsprechenden Coordinaten h_t einer jeden *ganzen* Zahl ω des Körpers nothwendig *ganze* rationale Zahlen sein müssen. Eine solche Basis $\omega_1, \omega_2 \ldots \omega_n$ wollen wir eine *Grundreihe* des Körpers Ω nennen; aus ihr ergeben sich alle anderen Grundreihen desselben Körpers, wenn man n ganze Zahlen ω von der Form (1) so wählt, dass die aus den n^2 zugehörigen Coordinaten gebildete Determinante $= \pm 1$ wird.

Die wichtigste Rolle spielt aber die Minimaldiscriminante selbst, sowohl hinsichtlich der inneren*) Constitution des Körpers Ω, als auch hinsichtlich seiner Verwandtschaft mit anderen Körpern**); wir wollen daher diese positive oder negative ganze rationale Zahl die *Grundzahl* oder die *Discriminante des Körpers* Ω nennen und mit $\Delta(\Omega)$ bezeichnen; sie ist offenbar zugleich die Grundzahl eines jeden mit Ω conjugirten Körpers.

Die Zahlen eines quadratischen Körpers sind z. B. von der Form $t + u\sqrt{D}$, wo t, u alle rationalen Zahlen durchlaufen, und D eine ganze rationale Zahl bedeutet, welche kein Quadrat und auch durch kein Quadrat ausser 1 theilbar ist. Ist $D \equiv 1 \pmod 4$, so bilden die Zahlen 1 und $\frac{1}{2}(1 + \sqrt{D})$ eine Grundreihe des Körpers, und seine Grundzahl ist $= D$; ist dagegen $D \equiv 2$ oder $\equiv 3 \pmod 4$, so bilden die Zahlen 1 und $\sqrt{D}$ eine Grundreihe des Körpers, und seine Grundzahl ist $= 4D$.

---

*) Vergl. *Kronecker: Ueber die algebraisch auflösbaren Gleichungen* (Monatsbericht der Berliner Ak. 14. April 1856).

**) Die erste Spur dieser Beziehungen hat sich bei einer schönen Untersuchung von *Kronecker* gezeigt (*Mémoire sur les facteurs irréductibles de l'expression* $x^n - 1$; Journ. de Math., p. p. Liouville; T. XIX. 1854). Um den Charakter dieser Gesetze, deren Entwicklung ich mir auf eine andere Gelegenheit verspare, näher anzudeuten, führe ich nur das einfachste Beispiel an: das kleinste gemeinschaftliche Multiplum zweier von einander verschiedenen quadratischen Körper A, B ist ein biquadratischer Körper K, der noch einen dritten quadratischen Körper C zum Divisor hat; die Grundzahl von K ist gleich dem Product aus den Grundzahlen von A, B, C, und zwar eine Quadratzahl.

Ist ferner θ eine primitive Wurzel der Gleichung $\theta^m = 1$ (§. 139), wo $m > 2$, so bilden die Zahlen $1, \theta, \theta^2 \ldots \theta^{n-1}$ die Grundreihe eines Körpers vom Grade $n = \varphi(m)$, dessen Grundzahl

$$\left(\frac{m\sqrt{-1}}{\sqrt[a-1]{a}\,\sqrt[b-1]{b}\,\sqrt[c-1]{c}\ldots}\right)^n$$

ist, wo $a, b, c \ldots$ alle verschiedenen in m aufgehenden Primzahlen bedeuten. Ist $m = 3$ (oder $= 6$), so ist dieser Körper ein quadratischer, seine Grundzahl $= -3$; ist $m = 4$, so ist die Grundzahl des quadratischen Körpers $= -4$.

2. Aus den vorstehenden Principien ergiebt sich leicht der folgende Fundamentalsatz:

Ist μ eine von Null verschiedene ganze Zahl des Körpers Ω, so ist die Anzahl der nach dem Modul μ incongruenten ganzen Zahlen des Körpers gleich dem absoluten Werth der Norm des Moduls μ.

Es sei $\mathfrak{m}$ das System aller durch μ theilbaren ganzen Zahlen (welche sich durch Addition und Subtraction reproduciren), und $\mathfrak{o}$ das System *aller* ganzen Zahlen des Körpers Ω, d. h. aller Zahlen ω von der Form (1), wo die Zahlen ω_ι eine *Grundreihe* des Körpers bilden, und die Coordinaten h_ι beliebige ganze rationale Zahlen bedeuten; da jeder Quotient $\omega : \mu$ (zufolge §. 160, 5.) durch Multiplication mit einer von Null verschiedenen ganzen rationalen Zahl in eine ganze Zahl verwandelt werden kann, so ist die Untersuchung des vorigen Paragraphen auf unsern Fall anwendbar. Mithin sind alle durch μ theilbaren Zahlen α des Systems $\mathfrak{o}$ von der Form

$$\alpha = \sum x_\iota \alpha_\iota = \mu \sum x_\iota \beta_\iota,$$

wo die n Zahlen $\alpha_\iota = \mu\beta_\iota$ particuläre Zahlen α bedeuten, also die Zahlen β_ι in $\mathfrak{o}$ enthalten sind, und die Grössen x_ι alle rationalen ganzen Zahlwerthe annehmen dürfen; die Anzahl der *Classen*, in welche das System $\mathfrak{o}$ in Bezug auf den Modul μ zerfällt, ist ferner gleich der aus den Coordinaten der n Zahlen $\alpha_1, \alpha_2 \ldots \alpha_n$ gebildeten Determinante Δ. Zugleich ist (nach §. 159, (11), (12))

$$\Delta(\alpha_1 \ldots \alpha_n) = a^2 \Delta(\Omega) = N(\mu)^2 \Delta(\beta_1 \ldots \beta_n);$$

da nun jede durch μ theilbare Zahl $\alpha = \mu\omega$ des Systems $\mathfrak{o}$ die Form $\mu \sum x_\iota \beta_\iota$ besitzt, so ist jede Zahl ω des Systems $\mathfrak{o}$ auch von der Form $\sum x_\iota \beta_\iota$; mithin bilden die Zahlen β_ι ebenfalls eine *Grund-*

reihe des Körpers, und folglich ist $\Delta(\beta_1 \ldots \beta_n) = \Delta(\Omega)$, also $a = \pm N(\mu)$, was zu beweisen war.

Zugleich leuchtet ein, dass nach der Methode des vorigen Paragraphen ein System von a incongruenten Repräsentanten der verschiedenen Classen, also ein *vollständiges Restsystem für den Modul* μ aufgestellt werden kann*).

3. Will man jetzt zwei gegebene ganze Zahlen θ, μ darauf prüfen, ob sie relative Primzahlen sind, so braucht man offenbar ω nur ein vollständiges Restsystem (mod. μ) durchlaufen zu lassen und nachzusehen, wie oft $\theta\omega \equiv 0 \pmod{\mu}$ wird; zeigt sich, dass dies nur dann eintritt, wenn $\omega \equiv 0 \pmod{\mu}$ ist, so ist also jede durch θ und μ theilbare ganze Zahl $\theta\omega$ auch theilbar durch $\theta\mu$, mithin sind θ, μ relative Primzahlen; besitzt aber die Congruenz $\theta\omega \equiv 0 \pmod{\mu}$ auch eine Wurzel ω, welche nicht $\equiv 0 \pmod{\mu}$ ist, so ist die entsprechende Zahl $\theta\omega$ durch θ und μ, aber nicht durch $\theta\mu$ theilbar, mithin sind θ, μ keine relative Primzahlen.

Ist θ relative Primzahl zu μ (z. B. $\theta = 1$), so durchläuft $\theta\omega$ gleichzeitig mit ω ein vollständiges Restsystem (mod. μ); folglich hat jede Congruenz $\theta\omega \equiv \theta' \pmod{\mu}$ immer eine und nur eine Wurzel ω (vergl. §. 22); ist ferner $\psi(\mu)$ die Anzahl aller Classen, deren Zahlen relative Primzahlen zum Modul μ sind, so durchläuft $\theta\omega$ gleichzeitig mit ω die Repräsentanten aller dieser Classen, und da das Product dieser Zahlen ω auch relative Primzahl zu μ ist, so ergiebt sich der Satz

$$\theta^{\psi(\mu)} \equiv 1 \pmod{\mu},$$

welcher dem Fermat'schen Satze (§. 19) entspricht.

4. Verfolgt man diese Analogie mit der rationalen Zahlentheorie weiter, so drängt sich immer wieder die Frage nach der Zusammensetzung der Zahlen des Systems $\mathfrak{o}$ (d. h. der ganzen Zahlen des Körpers Ω) aus Factoren auf, welche demselben System $\mathfrak{o}$ an-

*) Bilden die n Zahlen ω, *irgend* eine Basis des Körpers Ω, und ist $\mathfrak{o}$ das System aller der Zahlen ω von der Form (1), deren Coordinaten *ganze* Zahlen sind, so reproduciren sich die Zahlen des Systems $\mathfrak{o}$ durch Addition und Subtraction; nimmt man ferner an, dass sie sich auch durch Multiplication reproduciren, woraus zugleich folgt, dass sie *ganze* Zahlen sind, und nennt man zwei solche Zahlen ω, ω' stets und nur dann congruent in Bezug auf eine dritte solche Zahl μ, wenn der Quotient $(\omega - \omega') : \mu$ wieder eine Zahl des Systems $\mathfrak{o}$ ist, so ist die Anzahl der in $\mathfrak{o}$ enthaltenen, nach μ incongruenten Zahlen ebenfalls $= \pm N(\mu)$. Vergl. §. 165, 4.

gehören, und es zeigt sich zunächst, dass die unbegrenzte Zerlegbarkeit der ganzen Zahlen, wie sie in dem unendlichen Körper *aller* algebraischen Zahlen auftrat (§. 160, 7.), in einem endlichen Körper Ω wieder verschwindet. Dafür tritt aber bei unendlich vielen solchen Körpern Ω ein höchst eigenthümliches Phänomen auf, das schon früher (§. 16) gelegentlich erwähnt ist*). Nennt man eine Zahl in $\mathfrak{o}$ *zerlegbar*, wenn sie das Product aus zwei Zahlen in $\mathfrak{o}$ ist, welche beide keine Einheiten sind, dagegen *unzerlegbar*, wenn dies nicht der Fall ist, so ist offenbar jede zerlegbare Zahl μ darstellbar als Product aus einer *endlichen* Anzahl von unzerlegbaren Zahlen (vergl. §. 8), weil die Norm von μ gleich dem Producte aus den Normen der einzelnen Factoren ist (§. 159); aber es zeigt sich häufig, dass diese Zerlegung nicht eine vollkommen bestimmte ist, sondern dass mehrere *wesentlich verschiedene* Zerlegungen derselben Zahl in unzerlegbare Factoren existiren (§. 160, 6.). Dies widerspricht so sehr dem in der rationalen Zahlentheorie herrschenden Begriffe des Primzahlcharakters (§. 8), dass wir deshalb eine unzerlegbare Zahl als solche noch nicht als Primzahl anerkennen wollen; wir suchen daher für den wahren Primzahlcharakter ein kräftigeres Kriterium als diese unzulängliche Unzerlegbarkeit aufzustellen, ähnlich wie früher bei dem Begriffe der relativen Primzahl (§. 160, 7.), indem wir die zu untersuchende Zahl μ nicht zerlegen, sondern ihr Verhalten als *Modul* betrachten:

Eine ganze Zahl μ, welche keine Einheit ist, soll eine Primzahl heissen, wenn jedes durch μ theilbare Product $\eta\varrho$ wenigstens einen durch μ theilbaren Factor η oder ϱ besitzt.

Es ergiebt sich dann sofort, dass die höchste in einem Producte aufgehende Potenz einer Primzahl μ das Product aus den höchsten in den einzelnen Factoren aufgehenden Potenzen von μ,

*) Das dortige Beispiel passt freilich nicht ganz hierher, insofern die ganzen Zahlen des der Gleichung $\varrho^2 = -11$ entsprechenden quadratischen Körpers nicht durch die Form $t + u\varrho$, wohl aber durch die Form $t + u\theta$ erschöpft werden, wo $2\theta = 1 + \varrho$ ist; die Zahlen 3, 5, $2 + \varrho$, $2 - \varrho$ sind in der That zerlegbar: $3 = \theta(1-\theta)$, $5 = (1+\theta)(2-\theta)$, $2 - \varrho = -\theta(1+\theta)$, $2 + \varrho = -(1-\theta)(2-\theta)$; die vier Zahlen θ, $1-\theta$, $1+\theta$, $2-\theta$ sind Primzahlen in diesem Körper. Die in Rede stehende Erscheinung tritt aber in dem der Gleichung $x^2 = -5$ entsprechenden quadratischen Körper an dem Beispiel $3 \cdot 7 = (1+2x)(1-2x)$ wirklich auf (vergl. §. 71; die beiden Zahlen 3, 7 sind durch die Hauptform der Determinante -5 nicht darstellbar).

und dass jede durch μ nicht theilbare Zahl relative Primzahl zu μ ist. Man erkennt ferner leicht, dass die kleinste durch μ theilbare rationale ganze Zahl p nothwendig eine Primzahl (im Körper der rationalen Zahlen), und folglich die Norm von μ eine Potenz von p, nämlich ein rationaler Divisor von $N(p) = p^n$ sein muss. Es werden daher gewiss alle Primzahlen μ des Körpers Ω entdeckt, wenn die Divisoren aller rationalen Primzahlen p aufgesucht werden.

5. Ist aber μ keine Primzahl (und auch keine Einheit), existiren also zwei durch μ nicht theilbare Zahlen η, ϱ, deren Product $\eta\varrho$ durch μ theilbar ist, so schreiten wir zu einer Zerlegung von μ in wirkliche oder *ideale*, d. h. fingirte Factoren. Giebt es nämlich in $\mathfrak{o}$ einen grössten gemeinschaftlichen Theiler ν der beiden Zahlen η und $\mu = \nu\mu'$, der Art, dass die Quotienten $\eta : \nu$ und $\mu : \nu$ relative Primzahlen sind, so ist μ in die beiden Factoren ν und μ' zerlegt, von denen keiner eine Einheit ist, weil weder ϱ noch η durch μ theilbar ist. Der Factor μ' ist wesentlich dadurch bestimmt, dass alle Wurzeln α' der Congruenz $\eta\alpha' \equiv 0 \pmod{\mu}$ durch μ' theilbar sind (z. B. auch $\alpha' = \varrho$), und dass ebenso jede durch μ' theilbare Zahl α' auch der vorstehenden Congruenz genügt. Umgekehrt, giebt es in $\mathfrak{o}$ eine Zahl μ', welche in allen Wurzeln α' der Congruenz $\eta\alpha' \equiv 0 \pmod{\mu}$ und nur in diesen aufgeht, so ist auch μ theilbar durch μ', und der Quotient $\nu = \mu : \mu'$ ist der grösste gemeinschaftliche Theiler der beiden Zahlen η und μ.

Aber es kann sehr wohl der Fall eintreten, dass in $\mathfrak{o}$ keine solche Zahl μ' zu finden ist; als nun diese Erscheinung (bei den aus Einheitswurzeln gebildeten Zahlen) *Kummer* entgegentrat, so kam er auf den glücklichen Gedanken, trotzdem eine solche Zahl μ' zu fingiren und dieselbe als *ideale Zahl* einzuführen; die *Theilbarkeit* einer Zahl α' durch diese ideale Zahl μ' besteht lediglich darin, dass α' eine Wurzel der Congruenz $\eta\alpha' \equiv 0 \pmod{\mu}$ ist, und da diese idealen Zahlen in der Folge immer nur als Theiler oder Moduln auftreten, so hat diese Art ihrer Einführung durchaus keine Bedenken. Allein die Befürchtung, dass die unmittelbare Uebertragung der bei den *wirklichen* Zahlen üblichen Benennungen auf die idealen Zahlen im Anfang leicht Misstrauen gegen die Sicherheit der Beweisführung einflössen könnte, veranlasst uns, die Untersuchung dadurch in ein anderes Gewand einzukleiden, dass wir immer ganze *Systeme* von wirklichen Zahlen betrachten.

§. 163.

Wir gründen die Theorie der in $\mathfrak{o}$ enthaltenen Zahlen, d. h. aller ganzen Zahlen des Körpers Ω, auf den folgenden neuen Begriff.

1. Ein System $\mathfrak{a}$ von unendlich vielen in $\mathfrak{o}$ enthaltenen Zahlen soll ein *Ideal* heissen, wenn es den beiden Bedingungen genügt:

I. Die Summe und die Differenz je zweier Zahlen in $\mathfrak{a}$ sind wieder Zahlen in $\mathfrak{a}$.

II. Jedes Product aus einer Zahl in $\mathfrak{a}$ und einer Zahl in $\mathfrak{o}$ ist wieder eine Zahl in $\mathfrak{a}$.

Ist α in $\mathfrak{a}$ enthalten, so sagen wir, α sei *theilbar durch* $\mathfrak{a}$, $\mathfrak{a}$ *gehe in* α *auf*, weil die Ausdrucksweise hierdurch an Leichtigkeit gewinnt. Wir nennen ferner zwei in $\mathfrak{o}$ enthaltene Zahlen ω, ω', deren Differenz durch $\mathfrak{a}$ theilbar ist, *congruent nach* $\mathfrak{a}$ (vergl. §. 161), und bezeichnen dies durch die Congruenz $\omega \equiv \omega' \pmod{\mathfrak{a}}$; solche Congruenzen dürfen (zufolge I.) addirt, subtrahirt und (zufolge II.) multiplicirt werden, wie Gleichungen. Da je zwei einer dritten congruente Zahlen auch einander congruent sind, so kann man alle Zahlen in *Classen* (mod. $\mathfrak{a}$) eintheilen, indem man je zwei congruente Zahlen in dieselbe, je zwei incongruente Zahlen in zwei verschiedene Classen wirft; da nun, wenn μ eine von Null verschiedene Zahl in $\mathfrak{a}$ bedeutet, je zwei nach μ congruente Zahlen (zufolge II.) auch nach $\mathfrak{a}$ congruent sind — woraus zugleich folgt, dass $\mathfrak{a}$ aus einer oder mehreren Classen (mod. μ) besteht — so ist (zufolge §. 162, 2.) die Anzahl der Classen (mod. $\mathfrak{a}$), in welche $\mathfrak{o}$ zerfällt, *endlich**). Wählt man aus jeder Classe ein Individuum als Repräsentanten, so bilden dieselben ein *vollständiges Restsystem* (mod. $\mathfrak{a}$); die Anzahl dieser Classen oder incongruenten Zahlen soll die *Norm* von $\mathfrak{a}$ heissen und mit $N(\mathfrak{a})$ bezeichnet werden.

Ist η eine von Null verschiedene Zahl in $\mathfrak{o}$, so bilden alle durch η theilbaren Zahlen in $\mathfrak{o}$ ein Ideal, welches mit $\mathfrak{i}(\eta)$ bezeichnet werden soll; solche Ideale sind besonders ausgezeichnet und sollen

*) Dasselbe ergiebt sich unmittelbar aus §. 161; ist nämlich ω irgend eine Zahl in $\mathfrak{o}$, so kann durch Multiplication mit einer von Null verschiedenen ganzen rationalen Zahl der Quotient $\omega : \mu$ in eine ganze Zahl, also ω (zufolge II.) in eine Zahl des Ideals $\mathfrak{a}$ verwandelt werden.

Hauptideale heissen; die Norm von $\mathfrak{i}(\eta)$ ist $= \pm N(\eta)$; ist η eine Einheit, so ist $\mathfrak{i}(\eta) = \mathfrak{o}$, und umgekehrt.

2. Wenn alle Zahlen eines Ideals $\mathfrak{a}$ auch in einem Ideal $\mathfrak{b}$ enthalten sind, so besteht offenbar $\mathfrak{b}$ aus einer oder mehreren Classen (mod. $\mathfrak{a}$), und wir wollen sagen, $\mathfrak{a}$ sei ein *Multiplum von* $\mathfrak{b}$ oder *theilbar durch* $\mathfrak{b}$, $\mathfrak{b}$ sei ein *Theiler von* $\mathfrak{a}$ oder *gehe in* $\mathfrak{a}$ *auf*.

Besteht $\mathfrak{b}$ aus r Classen (mod. $\mathfrak{a}$), so ist $N(\mathfrak{a}) = rN(\mathfrak{b})$. Durchläuft nämlich δ die Repräsentanten dieser r Classen, und γ ein vollständiges Restsystem (mod. $\mathfrak{b}$), so bilden die $rN(\mathfrak{b})$ Zahlen $\gamma + \delta$ ein vollständiges Restsystem (mod. $\mathfrak{a}$); denn erstens ist jede Zahl in $\mathfrak{o}$ congruent einer Zahl γ (mod. $\mathfrak{b}$), also $\equiv \gamma + \delta$ (mod. $\mathfrak{a}$), und zweitens folgt aus $\gamma + \delta \equiv \gamma' + \delta'$ (mod. $\mathfrak{a}$), wo γ', δ' ähnliche Bedeutung haben wie γ, δ, successive $\gamma + \delta \equiv \gamma' + \delta'$ (mod. $\mathfrak{b}$), $\gamma \equiv \gamma'$ (mod. $\mathfrak{b}$), $\gamma = \gamma'$, also $\delta \equiv \delta'$ (mod. $\mathfrak{a}$), $\delta = \delta'$, d. h. die sämmtlichen Zahlen $\gamma + \delta$ sind incongruent (mod. $\mathfrak{a}$).

Ein Ideal besitzt folglich nur eine *endliche* Anzahl von Theilern. Ist $\mathfrak{m}$ theilbar durch $\mathfrak{a}$, $\mathfrak{a}$ durch $\mathfrak{b}$, so ist auch $\mathfrak{m}$ durch $\mathfrak{b}$ theilbar. Das Hauptideal $\mathfrak{o}$ selbst geht in jedem Ideal auf und ist zugleich das *einzige* Ideal, welches die Zahl 1 oder überhaupt Einheiten enthält, und dessen Norm $= 1$ ist.

Das System aller derjenigen Zahlen, welche gleichzeitig in zwei Idealen $\mathfrak{a}$, $\mathfrak{b}$ enthalten sind, ist das *kleinste gemeinschaftliche Multiplum* $\mathfrak{m}$ von $\mathfrak{a}$, $\mathfrak{b}$, insofern jedes gemeinschaftliche Multiplum von $\mathfrak{a}$, $\mathfrak{b}$ durch das Ideal $\mathfrak{m}$ theilbar ist. Durchläuft α alle Zahlen in $\mathfrak{a}$, β alle Zahlen in $\mathfrak{b}$, so ist das System aller Zahlen $\alpha + \beta$ der *grösste gemeinschaftliche Theiler* $\mathfrak{d}$ der Ideale $\mathfrak{a}$, $\mathfrak{b}$, weil jeder gemeinschaftliche Theiler von $\mathfrak{a}$, $\mathfrak{b}$ in dem Ideale $\mathfrak{d}$ aufgeht*).

Ist r die Anzahl der in $\mathfrak{b}$ enthaltenen Zahlen, welche (mod. $\mathfrak{a}$) incongruent sind, so besteht $\mathfrak{b}$ aus r Classen (mod. $\mathfrak{m}$), und $\mathfrak{b}$ aus r Classen (mod. $\mathfrak{a}$); also ist $N(\mathfrak{m}) = rN(\mathfrak{b})$, $N(\mathfrak{a}) = rN(\mathfrak{d})$, und $N(\mathfrak{m})N(\mathfrak{d}) = N(\mathfrak{a})N(\mathfrak{b})$.

Ist $\mathfrak{b}$ ein Hauptideal $= \mathfrak{i}(\eta)$, so ist die Anzahl r der in $\mathfrak{b}$ enthaltenen Zahlen $\beta = \eta\omega$, welche (mod. $\mathfrak{a}$) incongruent sind, zugleich die Norm des aus allen Wurzeln ϱ der Congruenz $\eta\varrho \equiv 0$ (mod. $\mathfrak{a}$) bestehenden Ideals $\mathfrak{r}$, weil zwei Zahlen ω, ω' stets und nur dann congruent (mod. $\mathfrak{r}$) sind, wenn $\eta\omega \equiv \eta\omega'$ (mod $\mathfrak{a}$) ist. Mithin ist in diesem Falle $N(\mathfrak{a}) = N(\mathfrak{r})N(\mathfrak{d})$.

*) Die Erweiterung dieser Definitionen von $\mathfrak{m}$ und $\mathfrak{d}$ für mehr als zwei Ideale $\mathfrak{a}, \mathfrak{b} \ldots$ liegt auf der Hand.

3. Ein von $\mathfrak{o}$ verschiedenes Ideal $\mathfrak{p}$, welches keinen von $\mathfrak{o}$ und $\mathfrak{p}$ verschiedenen Theiler besitzt, soll ein *Primideal* heissen. Dann gilt folgender Satz:

Ist $\eta\varrho \equiv 0$ (*mod.* $\mathfrak{p}$), *so ist wenigstens eine der beiden Zahlen* η, ϱ *durch* $\mathfrak{p}$ *theilbar.* Ist nämlich η nicht $\equiv 0$ (mod. $\mathfrak{p}$), so bilden die sämmtlichen Wurzeln ϱ der Congruenz $\eta\varrho \equiv 0$ (mod. $\mathfrak{p}$) offenbar ein in $\mathfrak{p}$ aufgehendes Ideal, welches, da es die Zahl 1 nicht enthält, von $\mathfrak{o}$ verschieden und folglich mit $\mathfrak{p}$ identisch ist, was zu beweisen war.

Dieser Satz ist charakteristisch für ein Primideal, da er sich folgendermaassen umkehren lässt: *Enthält jedes durch ein (von* $\mathfrak{o}$ *verschiedenes) Ideal* $\mathfrak{p}$ *theilbare Product mindestens einen durch* $\mathfrak{p}$ *theilbaren Factor, so ist* $\mathfrak{p}$ *ein Primideal.* Ist nämlich $\mathfrak{q}$ ein Theiler des Ideals $\mathfrak{p}$, aber verschieden von $\mathfrak{p}$, so giebt es in $\mathfrak{q}$ eine nicht in $\mathfrak{p}$ enthaltene Zahl ω; dann ist (zufolge der Annahme) auch keine der Potenzen $\omega^2, \omega^3 \ldots$ durch $\mathfrak{p}$ theilbar; da aber nur eine endliche Anzahl von incongruenten Zahlen (mod. $\mathfrak{p}$) existirt, so muss einmal für zwei *verschiedene* Exponenten m und $m+s > m$ nothwendig $\omega^{m+s} \equiv \omega^m$ (mod. $\mathfrak{p}$), also das Product $\omega^m(\omega^s - 1)$ durch $\mathfrak{p}$ theilbar sein; da nun ω^m nicht durch $\mathfrak{p}$ theilbar ist, so muss (zufolge der Annahme) der andere Factor $\omega^s - 1$ durch $\mathfrak{p}$, und folglich auch durch $\mathfrak{q}$ theilbar sein; nun ist ω und, weil $s > 0$ ist, auch $\omega^s \equiv 0$ (mod. $\mathfrak{q}$), mithin ist auch die Zahl 1 in $\mathfrak{q}$ enthalten, also $\mathfrak{q} = \mathfrak{o}$, was zu beweisen war.

Nennt man ein von $\mathfrak{o}$ verschiedenes Ideal *zusammengesetzt*, wenn es kein Primideal ist, so lässt sich dieser Satz auch so aussprechen: *Ist* $\mathfrak{a}$ *ein zusammengesetztes Ideal, so giebt es zwei durch* $\mathfrak{a}$ *nicht theilbare Zahlen* η, ϱ, *deren Product* $\eta\varrho$ *durch* $\mathfrak{a}$ *theilbar ist.* Wir beweisen ihn zum zweiten Male auf folgende Art. Es sei $\mathfrak{e}$ ein von $\mathfrak{a}$ und $\mathfrak{o}$ verschiedener Theiler von $\mathfrak{a}$, so giebt es in $\mathfrak{e}$ eine durch $\mathfrak{a}$ nicht theilbare Zahl η, und der grösste gemeinschaftliche Theiler $\mathfrak{b}$ von $\mathfrak{a}$ und $\mathfrak{i}(\eta)$ ist theilbar durch $\mathfrak{e}$, also von $\mathfrak{o}$ verschieden, mithin ist $N(\mathfrak{b}) > 1$. Das aus allen Wurzeln ϱ der Congruenz $\eta\varrho \equiv 0$ (mod. $\mathfrak{a}$) bestehende Ideal $\mathfrak{r}$ ist ein Theiler von $\mathfrak{a}$, und da (zufolge 2.) $N(\mathfrak{a}) = N(\mathfrak{r})N(\mathfrak{b}) > N(\mathfrak{r})$ ist, so ist $\mathfrak{r}$ verschieden von $\mathfrak{a}$ und enthält folglich eine durch $\mathfrak{a}$ nicht theilbare Zahl ϱ, was zu beweisen war.

Es leuchtet nun ein, dass die kleinste (von Null verschiedene) rationale Zahl p, welche in einem Primideale $\mathfrak{p}$ enthalten ist, nothwendig eine *Primzahl* (im rationalen Zahlkörper) sein muss; da

ferner $\mathfrak{p}$ in $\mathfrak{i}(p)$ aufgeht, so ist $N(\mathfrak{p})$ ein Theiler von $N(p) = p^n$, also ebenfalls eine Potenz $p^{f'}$ der rationalen Primzahl p, und man findet leicht (vergl. §. 162, 3.), dass jede in $\mathfrak{o}$ enthaltene Zahl ω der Congruenz

$$\omega^{p^{f'}} \equiv \omega \pmod{\mathfrak{p}}$$

genügt*). Auch hat es keine Schwierigkeit, die allgemeinen Sätze der §§. 26, 27, 29, 30, 31 auf Congruenzen in Bezug auf den Modul $\mathfrak{p}$ zu übertragen.

Ist das kleinste gemeinschaftliche Multiplum $\mathfrak{m}$ *der Ideale* $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ . . . *durch das Primideal* $\mathfrak{p}$ *theilbar, so geht* $\mathfrak{p}$ *wenigstens in einem der Ideale* $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ . . . *auf.* Ist nämlich *keins* dieser Ideale durch $\mathfrak{p}$ theilbar, giebt es also in $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ . . . resp. Zahlen α, β, γ . . ., die nicht durch $\mathfrak{p}$ theilbar sind, so ist das in $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ . . ., also auch in

*) Hierauf beruht das Eingreifen der *Theorie der höheren Congruenzen* (vergl. §. 26), welche zur Bestimmung der Primideale dient. Für die Körper vom Grade $n = \varphi(m)$, welche aus den primitiven Wurzeln θ der Gleichung $\theta^m = 1$ entspringen, ist dieselbe zuerst ausgeführt, und zwar von *Kummer*, dem Schöpfer der Theorie der idealen Zahlen; den hierauf bezüglichen Theil seiner Untersuchungen findet man am vollständigsten zusammengestellt in den Abhandlungen: *Mémoire sur la théorie des nombres complexes composés de racines de l'unité et de nombres entiers* (Journ. de Math. p. p. Liouville, T. XVI. 1851). — *Theorie der idealen Primfactoren der complexen Zahlen, welche aus den Wurzeln der Gleichung* $\omega^n = 1$ *gebildet sind, wenn* n *eine zusammengesetzte Zahl ist* (Abh. der Berliner Ak. 1856). Das Hauptresultat ergiebt sich mit grösster Leichtigkeit aus unserer Theorie und lautet in unserer Ausdrucksweise folgendermassen: Ist p eine rationale Primzahl und m' der grösste durch p nicht theilbare Divisor von $m = p'm'$, *gehört* ferner p zum Exponenten f (mod. m'), wo $\varphi(m') = ef$ (§. 28), so ist $\mathfrak{i}(p) = (\mathfrak{p}_1 \mathfrak{p}_2 \ldots \mathfrak{p}_e)^{\varphi(p')}$, wo $\mathfrak{p}_1$, $\mathfrak{p}_2$ . . . $\mathfrak{p}_e$ von einander verschiedene Primideale bedeuten, deren Normen $= p^f$ sind; wenn $p' > 1$, so ist $\mathfrak{i}(1 - \theta^{m'}) = \mathfrak{p}_1 \mathfrak{p}_2 \ldots \mathfrak{p}_e$. — Für complexe Zahlen einer höheren Stufe vergl. *Kummer: Ueber die allgemeinen Reciprocitätsgesetze unter den Resten und Nichtresten der Potenzen, deren Grad eine Primzahl ist* (Abh. der Berliner Ak. 1859). — Für diejenigen Körper Ω, deren conjugirte Körper mit Ω identisch sind, und welche ich *Galois'sche Körper* nennen möchte, vergl. *Selling: Ueber die idealen Primfactoren der complexen Zahlen, welche aus den Wurzeln einer beliebigen irreductibelen Gleichung rational gebildet sind* (Schlömilch's Zeitschr. für Math. u. Phys. Bd. 10. 1865). — Ein specieller Fall biquadratischer Körper ist vollständig durchgeführt von *Bachmann: Die Theorie der complexen Zahlen, welche aus zwei Quadratwurzeln zusammengesetzt sind.* 1867. — Für eine gewisse Classe cubischer Körper vergl. *Eisenstein: Allgemeine Untersuchungen über die Formen dritten Grades mit drei Variabeln, welche der Kreistheilung ihre Entstehung verdanken* (Crelle's Journ. XXVIII).

$\mathfrak{m}$ enthaltene Product $\alpha\beta\gamma\ldots$ nicht theilbar durch das Primideal $\mathfrak{p}$, und folglich geht $\mathfrak{p}$ *nicht* in $\mathfrak{m}$ auf, was zu beweisen war.

Ist die Zahl η nicht theilbar durch das Ideal $\mathfrak{a}$, so giebt es immer eine durch η theilbare Zahl ν der Art, dass alle Wurzeln π der Congruenz $\nu\pi \equiv 0$ (mod. $\mathfrak{a}$) ein Primideal bilden. Alle Wurzeln β der Congruenz $\eta\beta \equiv 0$ (mod. $\mathfrak{a}$) bilden ein in $\mathfrak{a}$ aufgehendes Ideal $\mathfrak{b}$, welches von $\mathfrak{o}$ verschieden ist, weil es die Zahl 1 nicht enthält; ist $\mathfrak{b}$ ein Primideal, so ist der Satz bewiesen. Ist $\mathfrak{b}$ kein Primideal, giebt es also zwei durch $\mathfrak{b}$ nicht theilbare Zahlen η', ϱ', deren Product $\eta'\varrho' \equiv 0$ (mod. $\mathfrak{b}$) ist, so bilden alle Wurzeln γ der Congruenz $\eta'\gamma \equiv 0$ (mod. $\mathfrak{b}$), d. h. der Congruenz $\eta\eta'\gamma \equiv 0$ (mod. $\mathfrak{a}$), ein in $\mathfrak{b}$ aufgehendes Ideal $\mathfrak{c}$, und zwar ist (zufolge 2.) $N(\mathfrak{c}) < N(\mathfrak{b})$, weil ϱ' in $\mathfrak{c}$, aber nicht in $\mathfrak{b}$ enthalten ist; ausserdem ist $\mathfrak{c}$ von $\mathfrak{o}$ verschieden, weil η' nicht in $\mathfrak{b}$, und folglich die Zahl 1 nicht in $\mathfrak{c}$ enthalten ist; ist $\mathfrak{c}$ ein Primideal, so ist der Satz bewiesen. Ist aber $\mathfrak{c}$ kein Primideal, so kann man in derselben Weise fortfahren; endlich muss in der Reihe der Ideale $\mathfrak{b}, \mathfrak{c}, \mathfrak{d}\ldots$, deren Normen immer kleiner werden, aber stets > 1 bleiben, ein Primideal $\mathfrak{p}$ auftreten, welches aus allen Wurzeln π der Congruenz $\nu\pi \equiv 0$ (mod. $\mathfrak{a}$) besteht, wo $\nu = \eta\eta'\eta''\ldots$ durch η theilbar ist.

4. Ist μ eine von Null verschiedene Zahl in $\mathfrak{o}$ und keine Einheit, so existirt zufolge des zuletzt bewiesenen Satzes (in welchem man $\eta = 1$ nehmen kann) jedenfalls eine Zahl ν der Art, dass alle Wurzeln π der Congruenz $\nu\pi \equiv 0$ (mod. μ) ein Primideal $\mathfrak{p}$ bilden; Primideale, welche aus den sämmtlichen Wurzeln einer solchen Congruenz bestehen, wollen wir vorläufig *einfache* Ideale nennen. Ist nun r irgend ein ganzer rationaler, nicht negativer Exponent, so bilden alle Wurzeln ϱ der Congruenz $\varrho\nu^r \equiv 0$ (mod. μ^r) ein Ideal, welches die $r$te *Potenz* von $\mathfrak{p}$ heissen und mit $\mathfrak{p}^r$ bezeichnet werden soll. Diese Definition ist unabhängig von dem zur Definition von $\mathfrak{p}$ benutzten Zahlenpaar μ, ν; ist nämlich μ' irgend eine von Null verschiedene, durch $\mathfrak{p}$ theilbare Zahl, also $\nu\mu' = \mu\nu'$, so folgt aus $\varrho\nu^r \equiv 0$ (mod. μ^r) durch Multiplication mit μ'^r und Division durch μ^r auch $\varrho\nu'^r \equiv 0$ (mod. μ'^r), und umgekehrt. Von der grössten Wichtigkeit sind aber die folgenden Sätze über einfache Ideale $\mathfrak{p}$:

Ist $s \geqq r$, so ist $\mathfrak{p}^s$ theilbar durch $\mathfrak{p}^r$. Ist nämlich σ in $\mathfrak{p}^s$ enthalten, also $\sigma\nu^s = \tau\mu^s$, so folgt, dass

$$\left(\frac{\sigma\nu^r}{\mu^r}\right)^s = \tau^r\sigma^{s-r}$$

eine ganze Zahl ist; mithin ist (nach §. 160, 3.) der jedenfalls dem Körper Ω angehörige Quotient $\sigma\nu^r : \mu^r$ ebenfalls eine *ganze* Zahl, also in $\mathfrak{o}$ enthalten, weil $\mathfrak{o}$ *alle* ganzen Zahlen des Körpers Ω umfasst*); also ist jede Zahl σ des Ideals $\mathfrak{p}^s$ auch in $\mathfrak{p}^r$ enthalten.

Ist ϱ eine von Null verschiedene Zahl in $\mathfrak{o}$, so giebt es immer eine höchste in ϱ aufgehende Potenz von $\mathfrak{p}$. Wäre nämlich für unendlich viele Exponenten r das Product $\varrho\nu^r$ theilbar durch μ^r, so müsste, da nur eine endliche Anzahl incongruenter Zahlen (mod. ϱ) existirt, für zwei *verschiedene* solche Exponenten r, s nothwendig einmal

$$\frac{\varrho\nu^r}{\mu^r} \equiv \frac{\varrho\nu^s}{\mu^s} \pmod{\varrho}, \quad \left(\frac{\nu}{\mu}\right)^r = \left(\frac{\nu}{\mu}\right)^s + \omega$$

werden, wo ω eine ganze Zahl; hieraus würde aber (nach §. 160, 3.) folgen, dass ν durch μ theilbar wäre, was nicht der Fall ist, weil sonst $\mathfrak{p} = \mathfrak{o}$ wäre.

Sind $\mathfrak{p}^r$, $\mathfrak{p}^s$ resp. die höchsten in ϱ, σ aufgehenden Potenzen, so ist $\mathfrak{p}^{r+s}$ die höchste in $\varrho\sigma$ aufgehende Potenz von $\mathfrak{p}$. Denn da $\varrho\nu^r = \varrho'\mu^r$, $\sigma\nu^s = \sigma'\mu^s$, und keins der Producte $\nu\varrho'$, $\nu\sigma'$ durch μ theilbar ist, so folgt $\varrho\sigma\nu^{r+s} = \varrho'\sigma'\mu^{r+s}$, und $\nu\varrho'\sigma'$ kann nicht durch μ theilbar sein, weil $\mathfrak{p}$ ein Primideal ist.

Ist $e \geqq 1$ der Exponent der höchsten in μ selbst aufgehenden Potenz von $\mathfrak{p}$, also $\mu\nu^e = \varkappa\mu^e$, wo $\nu\varkappa$ *nicht* theilbar durch μ, so folgt $\nu^e = \varkappa\mu^{e-1}$, d. h. der Exponent der höchsten in ν aufgehenden Potenz von $\mathfrak{p}$ ist $= e-1$. Das Ideal $\mathfrak{p}^e$ besteht aus den sämmtlichen Wurzeln θ der Congruenz $\varkappa\theta \equiv 0 \pmod{\mu}$. Die ganze Zahl $\lambda = \varkappa\mu : \nu = \sqrt[e]{\mu\varkappa^{e-1}}$ ist durch $\mathfrak{p}$, aber nicht durch $\mathfrak{p}^2$ theilbar; mithin ist λ^r durch $\mathfrak{p}^r$, aber nicht durch $\mathfrak{p}^{r+1}$ theilbar, woraus beiläufig folgt, dass die Ideale $\mathfrak{p}^r$ und $\mathfrak{p}^{r+1}$ wirklich *verschieden* sind. Endlich leuchtet folgender Satz ein:

Jede Potenz $\mathfrak{p}^r$ eines einfachen Ideals $\mathfrak{p}$ ist durch kein von $\mathfrak{p}$ verschiedenes Primideal theilbar. Ist nämlich π irgend eine Zahl in $\mathfrak{p}$, so muss ein in $\mathfrak{p}^r$ aufgehendes Primideal in π^r, also (zufolge 3.) in π selbst, d. h. in $\mathfrak{p}$ aufgehen und folglich mit $\mathfrak{p}$ identisch sein.

5. Die Wichtigkeit der einfachen Ideale und ihre Analogie mit den rationalen Primzahlen tritt unmittelbar hervor in dem folgenden Hauptsatz:

---

*) Sobald diese Bedingung nicht erfüllt ist, verlieren auch die obigen Sätze ihre *allgemeine* Gültigkeit; dies ist von Wichtigkeit für die Erweiterung der Definition der Ideale (vergl. §. 165, 4.).

Wenn alle in einer von Null verschiedenen Zahl μ aufgehenden Potenzen einfacher Ideale auch in einer Zahl η aufgehen, so ist η durch μ theilbar. Ist η *nicht* theilbar durch μ, so giebt es (zufolge 3.) eine durch η theilbare Zahl ν der Art, dass alle Wurzeln π der Congruenz $\nu\pi \equiv 0 \pmod{\mu}$ ein in μ aufgehendes einfaches Ideal $\mathfrak{p}$ bilden; ist $\mathfrak{p}^e$ die höchste in μ aufgehende Potenz, so ist (nach 4.) $\mathfrak{p}^{e-1}$ die höchste in ν aufgehende Potenz, und da ν durch η theilbar ist, so kann η *nicht* durch $\mathfrak{p}^e$ theilbar sein, was zu beweisen war. Derselbe Satz lässt sich offenbar auch so aussprechen: *Jedes Hauptideal* $\mathfrak{i}(\mu)$ *ist das kleinste gemeinschaftliche Multiplum aller in* μ *aufgehenden Potenzen von einfachen Idealen.* Es folgt zunächst:

Jedes Primideal $\mathfrak{p}$ *ist ein einfaches Ideal.* Es sei μ irgend eine von Null verschiedene Zahl in $\mathfrak{p}$, so muss $\mathfrak{p}$ (zufolge 3.) in einer der Potenzen einfacher Ideale aufgehen, deren kleinstes gemeinschaftliches Multiplum $\mathfrak{i}(\mu)$ ist; mithin ist $\mathfrak{p}$ selbst (zufolge 4.) ein einfaches Ideal. — Wir sprechen daher künftig nur noch von Primidealen, nicht mehr von einfachen Idealen.

Wenn alle in einem Ideal $\mathfrak{m}$ *aufgehenden Potenzen von Primidealen auch in einer Zahl* η *aufgehen, so ist* η *theilbar durch* $\mathfrak{m}$. Ist η *nicht* theilbar durch $\mathfrak{m}$, so giebt es (nach 3.) eine durch η theilbare Zahl ν der Art, dass alle Wurzeln π der Congruenz $\nu\pi \equiv 0 \pmod{\mathfrak{m}}$ ein Primideal $\mathfrak{p}$ bilden; ist $\mathfrak{p}^e$ die höchste in $\mathfrak{m}$ aufgehende Potenz von $\mathfrak{p}$, so giebt es in $\mathfrak{m}$ eine nicht durch $\mathfrak{p}^{e+1}$ theilbare Zahl μ, und das aus allen Wurzeln ϱ der Congruenz $\nu\varrho \equiv 0 \pmod{\mu}$ bestehende Ideal $\mathfrak{r}$ ist theilbar durch $\mathfrak{p}$, weil $\nu\varrho \equiv 0 \pmod{\mathfrak{m}}$ ist. Sind nun $\mathfrak{p}^e, \mathfrak{p}'^{e'}, \mathfrak{p}''^{e''} \ldots$ die sämmtlichen höchsten in μ aufgehenden Potenzen verschiedener Primideale $\mathfrak{p}, \mathfrak{p}', \mathfrak{p}'' \ldots$, so besteht $\mathfrak{r}$ zufolge des obigen Hauptsatzes aus allen gemeinschaftlichen Wurzeln ϱ der Congruenzen $\nu\varrho \equiv 0 \pmod{\mathfrak{p}^e}$, $\nu\varrho \equiv 0 \pmod{\mathfrak{p}'^{e'}}$, $\nu\varrho \equiv 0 \pmod{\mathfrak{p}''^{e''}}$ u. s. w., d. h. $\mathfrak{r}$ ist das kleinste gemeinschaftliche Multiplum der Ideale $\mathfrak{q}$, $\mathfrak{q}'$, $\mathfrak{q}'' \ldots$, welche resp. aus den Wurzeln jeder einzelnen dieser Congruenzen bestehen; da nun die Ideale $\mathfrak{q}', \mathfrak{q}'' \ldots$ als Theiler von $\mathfrak{p}'^{e'}, \mathfrak{p}''^{e''} \ldots$ nicht durch $\mathfrak{p}$ theilbar sind, so muss, weil $\mathfrak{r}$ durch $\mathfrak{p}$ theilbar ist, auch $\mathfrak{q}$ (zufolge 3.) durch $\mathfrak{p}$ theilbar sein; es kann folglich $\mathfrak{p}^e$ nicht in ν aufgehen (weil sonst $\mathfrak{q} = \mathfrak{o}$, also nicht durch $\mathfrak{p}$ theilbar wäre), und da ν durch η theilbar ist, so kann $\mathfrak{p}^e$ auch *nicht* in η aufgehen, was zu beweisen war.

Dieser *Fundamentalsatz* lässt sich offenbar auch so aussprechen: *Jedes Ideal ist das kleinste gemeinschaftliche Multiplum aller in ihm aufgehenden Potenzen von Primidealen.* Er entspricht durchaus

dem Fundamentalsatze der rationalen Zahlentheorie über die Zusammensetzung der Zahlen aus Primzahlen (§. 8); denn ihm zufolge ist jedes Ideal $\mathfrak{m}$ *vollständig bestimmt*, sobald die höchsten in $\mathfrak{m}$ aufgehenden Potenzen $\mathfrak{p}^e$, $\mathfrak{p}'^{e'}$, $\mathfrak{p}''^{e''}$ ... von Primidealen gegeben sind; aus ihm ergiebt sich auch ohne Weiteres der folgende Satz: *Ein Ideal* $\mathfrak{m}$ *ist stets und nur dann durch ein Ideal* $\mathfrak{b}$ *theilbar, wenn alle in* $\mathfrak{b}$ *aufgehenden Potenzen von Primidealen auch in* $\mathfrak{m}$ *aufgehen.* Dies folgt unmittelbar aus dem Begriffe des kleinsten gemeinschaftlichen Multiplums.

Ist $\mathfrak{m}$ *das kleinste gemeinschaftliche Multiplum von* $\mathfrak{p}^e$, $\mathfrak{p}'^{e'}$, $\mathfrak{p}''^{e''}$ ..., *wo* $\mathfrak{p}$, $\mathfrak{p}'$, $\mathfrak{p}''$ ... *von einander verschiedene Primideale bedeuten, so ist* $N(\mathfrak{m}) = N(\mathfrak{p})^e N(\mathfrak{p}')^{e'} N(\mathfrak{p}'')^{e''} \ldots$ Es giebt immer (zufolge 4.) eine durch $\mathfrak{p}^{e-1}$, aber nicht durch $\mathfrak{a} = \mathfrak{p}^e$ theilbare Zahl η; das aus allen Wurzeln ϱ der Congruenz $\eta\varrho \equiv 0$ (mod. $\mathfrak{a}$) bestehende Ideal $\mathfrak{r}$ ist verschieden von $\mathfrak{o}$ (weil es die Zahl 1 nicht enthält) und ein Theiler von $\mathfrak{p}$ (zufolge 4.), folglich identisch mit $\mathfrak{p}$; da ferner der grösste gemeinschaftliche Theiler $\mathfrak{d}$ der Ideale $\mathfrak{a} = \mathfrak{p}^e$ und $\mathfrak{i}(\eta)$ zufolge des eben bewiesenen Fundamentalsatzes $= \mathfrak{p}^{e-1}$ ist, so folgt (aus 2.) $N(\mathfrak{a}) = N(\mathfrak{r})\,N(\mathfrak{d})$, d. h. $N(\mathfrak{p}^e) = N(\mathfrak{p})\,N(\mathfrak{p}^{e-1})$, und hieraus allgemein $N(\mathfrak{p}^e) = N(\mathfrak{p})^e$. — Nun ist (zufolge der Definition 2.) das kleinste gemeinschaftliche Multiplum $\mathfrak{m}$ der Ideale $\mathfrak{p}^e$, $\mathfrak{p}'^{e'}$, $\mathfrak{p}''^{e''}$ ... zugleich auch das der Ideale $\mathfrak{a} = \mathfrak{p}^e$ und $\mathfrak{b}$, wo $\mathfrak{b}$ das kleinste gemeinschaftliche Multiplum der Ideale $\mathfrak{p}'^{e'}$, $\mathfrak{p}''^{e''}$ ... bedeutet; da ferner (zufolge des Fundamentalsatzes) $\mathfrak{o}$ der grösste gemeinschaftliche Theiler von $\mathfrak{a}$ und $\mathfrak{b}$ ist, so folgt (aus 2.) $N(\mathfrak{m}) = N(\mathfrak{a})\,N(\mathfrak{b})$, d. h. $N(\mathfrak{m}) = N(\mathfrak{p})^e N(\mathfrak{b})$ und hieraus ergiebt sich offenbar der zu beweisende Satz.

6. Multiplicirt man alle Zahlen eines Ideals $\mathfrak{a}$ mit allen Zahlen eines Ideals $\mathfrak{b}$, so bilden diese Producte und deren Summen ein durch $\mathfrak{a}$ und $\mathfrak{b}$ theilbares Ideal, welches das *Product aus den Factoren* $\mathfrak{a}$ *und* $\mathfrak{b}$ heissen und mit $\mathfrak{ab}$ bezeichnet werden soll. Aus dieser Erklärung leuchtet sofort ein, dass $\mathfrak{ao} = \mathfrak{a}$, $\mathfrak{ab} = \mathfrak{ba}$, ferner $(\mathfrak{ab})\mathfrak{c} = \mathfrak{a}(\mathfrak{bc})$ ist (vergl. §§. 1, 2, 147). Zugleich gilt folgender Satz:

Sind $\mathfrak{p}^a$, $\mathfrak{p}^b$ *resp. die höchsten in* $\mathfrak{a}$, $\mathfrak{b}$ *aufgehenden Potenzen des Primideals* $\mathfrak{p}$, *so ist* $\mathfrak{p}^{a+b}$ *die höchste in* $\mathfrak{ab}$ *aufgehende Potenz von* $\mathfrak{p}$; *und es ist* $N(\mathfrak{ab}) = N(\mathfrak{a})\,N(\mathfrak{b})$.

Aus der Erklärung folgt nämlich unmittelbar (mit Rücksicht auf 4.), dass $\mathfrak{ab}$ durch $\mathfrak{p}^{a+b}$ theilbar ist; da ferner in $\mathfrak{a}$ eine durch $\mathfrak{p}^{a+1}$ nicht theilbare Zahl α, in $\mathfrak{b}$ eine durch $\mathfrak{p}^{b+1}$ nicht theilbare

Zahl β existirt, so giebt es in $\mathfrak{a}\mathfrak{b}$ eine durch $\mathfrak{p}^{a+b+1}$ nicht theilbare Zahl $\alpha\beta$, womit der erste Theil des Satzes bewiesen ist. Ist also $\mathfrak{a}$ das kleinste gemeinschaftliche Multiplum der Potenzen $\mathfrak{p}^a$, $\mathfrak{p}'^{a'}$, $\mathfrak{p}''^{a''}$ ... der von einander verschiedenen Primideale $\mathfrak{p}$, $\mathfrak{p}'$, $\mathfrak{p}''$ ..., und $\mathfrak{b}$ das kleinste gemeinschaftliche Multiplum der Potenzen $\mathfrak{p}^b$, $\mathfrak{p}'^{b'}$, $\mathfrak{p}''^{b''}$..., so ist $\mathfrak{a}\mathfrak{b}$ dasjenige der Potenzen $\mathfrak{p}^{a+b}$, $\mathfrak{p}'^{a'+b'}$, $\mathfrak{p}''^{a''+b''}$..., woraus (mit Rücksicht auf 5.) auch der zweite Theil des Satzes folgt.

Da aus diesem Satze auch $\mathfrak{p}^a\mathfrak{p}^b = \mathfrak{p}^{a+b}$ folgt, so ist die oben (in 4.) gewählte Ausdrucks- und Bezeichnungsweise gerechtfertigt. Sind ferner $\mathfrak{p}$, $\mathfrak{p}'$, $\mathfrak{p}''$ ... von einander verschiedene Primideale, so ist $\mathfrak{p}^a\mathfrak{p}'^{a'}\mathfrak{p}''^{a''}$ ... das kleinste gemeinschaftliche Multiplum der Potenzen $\mathfrak{p}^a$, $\mathfrak{p}'^{a'}$, $\mathfrak{p}''^{a''}$ ... Auch leuchtet ein, dass der Begriff der Potenz durch die Definition $\mathfrak{a}^{r+1} = \mathfrak{a}\mathfrak{a}^r$ auf jedes Ideal $\mathfrak{a}$ ausgedehnt werden kann. Ist endlich $\mathfrak{a}$ *theilbar* durch $\mathfrak{b}$, so giebt es immer ein und nur ein Ideal $\mathfrak{r}$ der Art, dass $\mathfrak{a} = \mathfrak{r}\mathfrak{b}$ wird; sind nämlich $\mathfrak{p}^a$, $\mathfrak{p}^d$ die höchsten resp. in $\mathfrak{a}$, $\mathfrak{b}$ aufgehenden Potenzen eines Primideals $\mathfrak{p}$, so ist $d \leqq a$, und $\mathfrak{r}$ ist das Product aus allen Potenzen $\mathfrak{p}^{a-d}$. Mit Rücksicht hierauf erkennt man leicht, dass die früheren Sätze (in 2.) sich jetzt einfacher aussprechen lassen.

7. Wir nennen nun $\mathfrak{a}$ und $\mathfrak{b}$ *relative Primideale*, wenn ihr grösster gemeinschaftlicher Theiler $= \mathfrak{o}$ ist; ebenso soll η *relative Primzahl zum Ideal* $\mathfrak{a}$ heissen, wenn $\mathfrak{a}$ und $\mathfrak{i}(\eta)$ relative Primideale sind. Es leuchtet dann ein, dass die Sätze der rationalen Zahlentheorie über relative Primzahlen sich leicht auf die Theorie der Ideale übertragen lassen; wir begnügen uns aber hier, folgenden wichtigen Satz zu beweisen (vergl. §. 25):

Sind $\mathfrak{a}$, $\mathfrak{b}$ *relative Primideale, und* μ, ν *zwei gegebene Zahlen, so giebt es immer eine und nur eine Classe von Zahlen* η *(mod.* $\mathfrak{a}\mathfrak{b}$*), welche den Bedingungen* $\eta \equiv \mu$ *(mod.* $\mathfrak{a}$*),* $\eta \equiv \nu$ *(mod.* $\mathfrak{b}$*) genügen.* Durchlaufen nämlich μ, ν, η vollständige Restsysteme resp. für die drei Moduln $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{a}\mathfrak{b}$, so entspricht jeder Zahl η eine und nur eine Combination μ, ν der Art, dass $\mu \equiv \eta$ (mod. $\mathfrak{a}$), $\nu \equiv \eta$ (mod. $\mathfrak{b}$) ist; entspräche ferner zwei verschiedenen Zahlen η, η' des Restsystems für den Modul $\mathfrak{a}\mathfrak{b}$ eine und dieselbe Combination μ, ν, so wäre $\eta - \eta'$ theilbar sowohl durch $\mathfrak{a}$ als durch $\mathfrak{b}$, also auch durch $\mathfrak{a}\mathfrak{b}$ (weil $\mathfrak{a}$, $\mathfrak{b}$ relative Primideale sind), mithin wäre $\eta \equiv \eta'$ (mod. $\mathfrak{a}\mathfrak{b}$), was gegen die Voraussetzung streitet. Durchläuft daher η alle seine Werthe, deren Anzahl $= N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a})N(\mathfrak{b})$ ist, so entstehen ebensoviele *verschiedene* Combinationen μ, ν; und da genau ebensoviele ver-

schiedene Combinationen μ, ν wirklich existiren, so muss auch umgekehrt jede Combination μ, ν einer Zahl η entsprechen, was zu beweisen war.

Bedeutet $\psi(\mathfrak{a})$ die Anzahl der (mod. $\mathfrak{a}$) incongruenten relativen Primzahlen zu $\mathfrak{a}$, so ist $\psi(\mathfrak{ab}) = \psi(\mathfrak{a})\psi(\mathfrak{b})$, wenn $\mathfrak{a}$, $\mathfrak{b}$ relative Primideale bedeuten. Ist ferner $\mathfrak{p}$ ein Primideal, und $e \geqq 1$, so ist $\psi(\mathfrak{p}^e) = N(\mathfrak{p}^e) - N(\mathfrak{p}^{e-1}) = N(\mathfrak{p})^{e-1}(N(\mathfrak{p}) - 1)$; denn, wenn δ alle r durch $\mathfrak{p}$ theilbaren und nach dem Modul $\mathfrak{p}^e$ incongruenten Zahlen, wenn ferner γ ein vollständiges Restsystem (mod. $\mathfrak{p}$) durchläuft, so bilden die Zahlen $\gamma + \delta$ (zufolge 2.) ein vollständiges Restsystem (mod. $\mathfrak{p}^e$), und es ist $N(\mathfrak{p}^e) = rN(\mathfrak{p})$, also $r = N(\mathfrak{p}^{e-1})$; nun ist aber eine solche Zahl $\gamma + \delta$ stets und nur dann relative Primzahl zu $\mathfrak{p}^e$, wenn γ nicht $\equiv 0$ (mod. $\mathfrak{p}$) ist, und folglich ist die Anzahl der Zahlen $\gamma + \delta$, welche relative Primzahlen zu $\mathfrak{p}^e$ sind, gleich $r(N(\mathfrak{p}) - 1)$, was zu beweisen war.

Bedeutet $\mathfrak{p}$ ein Primideal, so giebt es (zufolge 4.) immer eine Zahl λ, welche durch $\mathfrak{p}$, aber nicht durch $\mathfrak{p}^2$ theilbar ist, mithin auch eine Zahl λ^e, welche durch $\mathfrak{p}^e$, aber nicht durch $\mathfrak{p}^{e+1}$ theilbar ist. Sind nun $\mathfrak{p}$, $\mathfrak{p}'$, $\mathfrak{p}''$ ... von einander verschiedene Primideale, und haben λ', λ'' ... ähnliche Bedeutung für $\mathfrak{p}'$, $\mathfrak{p}''$ ..., wie λ für $\mathfrak{p}$, so existirt immer, wenn e, e', e'' ... gegebene Exponenten bedeuten, eine Zahl η, welche den gleichzeitigen Congruenzen

$$\eta \equiv \lambda^e \pmod{\mathfrak{p}^{e+1}}, \quad \eta \equiv \lambda'^{e'} \pmod{\mathfrak{p}'^{e'+1}},$$
$$\eta \equiv \lambda''^{e''} \pmod{\mathfrak{p}''^{e''+1}} \ldots$$

genügt, weil die Moduln relative Primideale sind. Dann ist offenbar $\mathfrak{i}(\eta) = \mathfrak{m}\mathfrak{p}^e\mathfrak{p}'^{e'}\mathfrak{p}''^{e''} \ldots$, und das Ideal $\mathfrak{m}$ ist durch keines der Primideale $\mathfrak{p}$, $\mathfrak{p}'$, $\mathfrak{p}''$ theilbar. Hieraus folgt unmittelbar der Satz:

Sind $\mathfrak{a}$, $\mathfrak{b}$ *zwei beliebige Ideale, so giebt es immer ein solches relatives Primideal* $\mathfrak{m}$ *zu* $\mathfrak{b}$, *dass* $\mathfrak{am}$ *ein Hauptideal wird.* Sind nämlich $\mathfrak{p}$, $\mathfrak{p}'$, $\mathfrak{p}''$ ... alle von einander verschiedenen in $\mathfrak{ab}$ aufgehenden Primideale, und ist $\mathfrak{a} = \mathfrak{p}^e\mathfrak{p}'^{e'}\mathfrak{p}''^{e''} \ldots$ (wo die Exponenten $e, e', e'' \ldots$ auch $= 0$ sein können), so giebt es, wie eben gezeigt ist, ein durch $\mathfrak{a}$ theilbares Hauptideal $\mathfrak{i}(\eta) = \mathfrak{am}$ der Art, dass $\mathfrak{b}$ und $\mathfrak{m}$ relative Primideale sind.

Hieraus folgt auch, dass jedes Ideal $\mathfrak{a}$, welches kein Hauptideal ist, immer als der grösste gemeinschaftliche Theiler von *zwei* Hauptidealen angesehen werden kann; hat man nämlich nach Belieben ein durch $\mathfrak{a}$ theilbares Hauptideal $\mathfrak{i}(\eta') = \mathfrak{ab}$ gewählt, so kann man immer ein zweites $\mathfrak{i}(\eta) = \mathfrak{am}$ so wählen, dass $\mathfrak{b}$ und $\mathfrak{m}$ re-

lative Primideale werden; die sämmtlichen Zahlen des Ideals $\mathfrak{a}$ sind dann von der Form $\eta\omega + \eta'\omega'$, wo ω, ω' alle Zahlen in $\mathfrak{o}$ durchlaufen.

§. 164.

Wir gehen nun zu einer Eintheilung der Ideale des Körpers Ω in *Classen* über, welche auf folgenden Grundlagen beruht.

1. Das System E aller Hauptideale besitzt folgende fundamentale Eigenschaften*).

I. *Jedes Product aus zwei Idealen in E ist wieder ein Ideal in E.* Denn es ist $\mathfrak{i}(\eta)\,\mathfrak{i}(\eta') = \mathfrak{i}(\eta\eta')$.

II. *Sind $\mathfrak{e}$ und $\mathfrak{e}\mathfrak{e}'$ Ideale in E, so ist auch $\mathfrak{e}'$ ein Ideal in E.* Ist nämlich $\mathfrak{e} = \mathfrak{i}(\eta)$, $\mathfrak{e}\mathfrak{e}' = \mathfrak{i}(\eta'')$, so ist η'' theilbar durch η, also $\eta'' = \eta\eta'$, woraus $\mathfrak{e}' = \mathfrak{i}(\eta')$ folgt.

III. *Ist $\mathfrak{a}$ ein beliebiges Ideal, so giebt es immer ein Ideal $\mathfrak{m}$ der Art, dass $\mathfrak{a}\mathfrak{m}$ ein Ideal in E wird.* Denn es sei η irgend eine von Null verschiedene Zahl in $\mathfrak{a}$, so ist das Ideal $\mathfrak{e} = \mathfrak{i}(\eta)$ theilbar durch $\mathfrak{a}$, und folglich existirt (nach §. 163, 6. oder 7.) ein Ideal $\mathfrak{m}$, welches der Bedingung $\mathfrak{a}\mathfrak{m} = \mathfrak{e}$ genügt.

Wir nennen nun zwei Ideale $\mathfrak{a}$, $\mathfrak{a}'$ *äquivalent*, wenn ein Ideal $\mathfrak{m}$ der Art existirt, dass beide Producte $\mathfrak{a}\mathfrak{m}$, $\mathfrak{a}'\mathfrak{m}$ dem System E angehören**). Sind ferner $\mathfrak{a}'$, $\mathfrak{a}''$ äquivalent, giebt es also ein Ideal $\mathfrak{m}'$ der Art, dass $\mathfrak{a}'\mathfrak{m}'$, $\mathfrak{a}''\mathfrak{m}'$ Ideale in E sind, so gehören, wenn $\mathfrak{a}'\mathfrak{m}\mathfrak{m}' = \mathfrak{m}''$ gesetzt wird, auch die Producte $\mathfrak{a}\mathfrak{m}'' = (\mathfrak{a}\mathfrak{m})(\mathfrak{a}'\mathfrak{m}')$ und $\mathfrak{a}''\mathfrak{m}'' = (\mathfrak{a}'\mathfrak{m})(\mathfrak{a}''\mathfrak{m}')$ dem System E an (zufolge I.), d. h. die

*) Diese drei Eigenschaften sind aber nicht charakteristisch für das System E der Hauptideale, sondern sie kommen auch anderen Systemen zu, für welche dann nothwendig dieselben Gesetze der Classification gelten. Giebt es z. B. in Ω keine Einheit, deren Norm $= -1$ ist, und nimmt man ein Ideal $\mathfrak{i}(\eta)$ nur dann in das System E auf, wenn $N(\eta)$ *positiv* ist, so hat auch dieses System E dieselben drei Eigenschaften (vergl. *Kronecker: Ueber die Classenanzahl der aus Wurzeln der Einheit gebildeten complexen Zahlen*; Monatsber. d. Berliner Ak. 23. Juli 1863). Ebenso könnte man in E alle Ideale einer ganzen *Gruppe* von Classen aufnehmen, z. B. alle diejenigen, welche dem Hauptgeschlecht angehören.

**) Diese Definition kann offenbar auch durch die folgende ersetzt werden: zwei Ideale $\mathfrak{a}$, $\mathfrak{a}'$ heissen äquivalent, wenn es zwei Ideale $\mathfrak{e}$, $\mathfrak{e}'$ in E giebt, welche der Bedingung $\mathfrak{a}\mathfrak{e}' = \mathfrak{a}'\mathfrak{e}$ genügen.

dem Ideale $\mathfrak{a}'$ äquivalenten Ideale $\mathfrak{a}$, $\mathfrak{a}''$ sind auch einander äquivalent. Hieraus allein folgt schon die Möglichkeit, alle Ideale in Classen einzutheilen: eine *Classe* ist der Inbegriff aller Ideale, welche einem bestimmten Ideal äquivalent sind.

Das System E selbst bildet eine solche Classe. Gehören nämlich $\mathfrak{e}$, $\mathfrak{e}'$, $\mathfrak{e}''$ diesem System an, so gilt (zufolge I.) dasselbe von den Producten $\mathfrak{e}\mathfrak{e}''$, $\mathfrak{e}'\mathfrak{e}''$, d. h. $\mathfrak{e}$, $\mathfrak{e}'$ sind äquivalent und gehören folglich in eine und dieselbe Classe. Sind umgekehrt $\mathfrak{e}$, $\mathfrak{e}'$ äquivalent, und gehört $\mathfrak{e}$ dem System E an, so gilt dasselbe von $\mathfrak{e}'$; denn, wenn $\mathfrak{e}$, $\mathfrak{e}\mathfrak{e}''$, $\mathfrak{e}'\mathfrak{e}''$ Ideale in E sind, so gehört (zufolge II.) auch $\mathfrak{e}''$, mithin auch $\mathfrak{e}'$ dem Systeme E an. Diese Classe E soll die *Hauptclasse* heissen.

Durchläuft nun $\mathfrak{a}$ alle Ideale einer Classe A, $\mathfrak{b}$ alle Ideale einer Classe B, so gehören alle Producte $\mathfrak{a}\mathfrak{b}$ einer und derselben Classe an, welche *aus A und B zusammengesetzt* heissen und mit AB bezeichnet werden soll; gehören nämlich $\mathfrak{a}\mathfrak{m}$, $\mathfrak{a}'\mathfrak{m}$, $\mathfrak{b}\mathfrak{n}$, $\mathfrak{b}'\mathfrak{n}$ der Hauptclasse E an, so gilt (zufolge I.) dasselbe von $(\mathfrak{a}\mathfrak{b})(\mathfrak{m}\mathfrak{n}) = (\mathfrak{a}\mathfrak{m})(\mathfrak{b}\mathfrak{n})$ und $(\mathfrak{a}'\mathfrak{b}')(\mathfrak{m}\mathfrak{n}) = (\mathfrak{a}'\mathfrak{m})(\mathfrak{b}'\mathfrak{n})$. Offenbar ist $AB = BA$, $(AB)C = A(BC)$ u. s. w. (vergl. §. 147).

Ist $\mathfrak{a}$ ein beliebiges Ideal, $\mathfrak{e}$ ein Ideal in E, so sind $\mathfrak{a}$ und $\mathfrak{a}\mathfrak{e}$ äquivalent; gehört nämlich $\mathfrak{a}\mathfrak{m}$ dem System E an, so gilt dasselbe von $(\mathfrak{a}\mathfrak{e})\mathfrak{m} = (\mathfrak{a}\mathfrak{m})\mathfrak{e}$. Hieraus folgt $AE = A$ (vergl. §. 148, 1.).

Da ferner jedes gegebene Ideal $\mathfrak{a}$ (zufolge III.) durch Multiplication mit einem Ideal $\mathfrak{m}$ in ein Ideal der Hauptclasse E verwandelt werden kann, so gehört zu jeder gegebenen Classe A auch eine *entgegengesetzte* Classe M (oder A^{-1}) der Art, dass $AM = E$ wird, und zwar nur eine einzige, weil aus $AM' = E$ auch $AM'M = EM$, d. h. $M' = M$ folgt. Allgemein ergiebt sich hieraus, dass aus $AB = AC$ stets $B = C$ folgt (vergl. §. 148, 2.).

2. Dass nun die Anzahl aller Idealclassen *endlich* ist, beruht auf einer tieferen Eigenschaft des Systems E aller Hauptideale, welche jetzt zu besprechen ist. Bilden die ganzen Zahlen ω_1, $\omega_2 \ldots \omega_n$ eine Grundreihe (oder irgend eine Basis) des Körpers Ω, und setzen wir (wie in §. 159) $\omega = \Sigma h_i\omega_i$, $H = N(\omega)$, so ist H eine homogene Function $n$ten Grades der Coordinaten h_i mit *ganzen* rationalen Coefficienten; bedeutet nun s die Summe der absoluten Werthe dieser Coefficienten, so besteht folgender Satz:

Ist $\mathfrak{a}$ irgend ein Ideal, so giebt es immer ein durch $\mathfrak{a}$ theilbares Hauptideal, dessen Norm $\leqq sN(\mathfrak{a})$ ist. Man gebe jeder der n Coordinaten h_i alle $(k+1)$ Werthe 0, 1, 2 ... k, wo $k \leqq \sqrt[n]{N(\mathfrak{a})} < k+1$;

da die Anzahl $(k+1)^n$ der so entstehenden ganzen Zahlen ω grösser als $N(\mathfrak{a})$ ist, so müssen zwei ungleiche von ihnen einander congruent (mod. $\mathfrak{a}$) sein; ihre Differenz η wird dann eine von Null verschiedene, durch $\mathfrak{a}$ theilbare Zahl, und da die absoluten Werthe ihrer Coordinaten den Werth k nicht übersteigen, so ist $N(\eta)$ absolut genommen $\leqq s k^n \leqq s N(\mathfrak{a})$; das Hauptideal $\mathfrak{i}(\eta)$ hat daher die geforderte Eigenschaft. Derselbe Satz kann offenbar auch so ausgesprochen werden: *Jedes Ideal* $\mathfrak{a}$ *kann in ein Hauptideal verwandelt werden durch Multiplication mit einem Ideal* $\mathfrak{m}$, *dessen Norm* $\leqq s$ *ist.*

Hierzu tritt folgende Ueberlegung. Durchläuft ϱ ein vollständiges Restsystem (mod. $\mathfrak{m}$), so nimmt auch $1+\varrho$ lauter incongruente Werthe an, woraus durch Addition leicht folgt, dass die Zahl $m = N(\mathfrak{m})$ durch $\mathfrak{m}$ theilbar, dass also $\mathfrak{m}$ ein Theiler des Hauptideals $\mathfrak{i}(m)$ ist. Da nun jedes Ideal nur eine endliche Anzahl von Theilern besitzt (§. 163, 2.), so giebt es auch nur eine endliche Anzahl von Idealen $\mathfrak{m}$, deren Normen einen gegebenen Werth m besitzen, mithin auch nur eine endliche Anzahl von Idealen $\mathfrak{m}$, deren Normen einen gegebenen Werth s nicht übertreffen. Zufolge des vorhergehenden Satzes giebt es daher eine *endliche* Anzahl von Idealen $\mathfrak{m}$ der Art, dass jedes beliebige Ideal $\mathfrak{a}$ durch Multiplication mit einem dieser Ideale $\mathfrak{m}$ in ein Hauptideal verwandelt werden kann; dieser wichtige Zusatz zu der Eigenschaft III. des Systems E kann offenbar auch so gefasst werden: *Die Anzahl der Idealclassen, d. h. die Anzahl der nicht äquivalenten Ideale ist endlich.*

3. Es leuchtet nun ein, dass alle Sätze über Perioden oder über Gruppen von Classen quadratischer Formen (§. 149) ohne Weiteres auf unsere Idealclassen übertragen werden können. Wir heben hier nur die einzige Folgerung hervor:

Jedes Ideal kann durch Potenzirung in ein Hauptideal verwandelt werden. Ist also $\mathfrak{a}$ ein Ideal, so giebt es immer einen positiven ganzen rationalen Exponenten m (Divisor der Classenanzahl) der Art, dass $\mathfrak{a}^m$ ein Hauptideal $\mathfrak{i}(\eta)$ wird; ist nun α irgend eine Zahl des Ideals $\mathfrak{a}$, so ist α^m theilbar durch η, mithin α theilbar durch die ganze Zahl $\sqrt[m]{\eta}$ (§. 160, 3.). Ist $\mathfrak{p}^e$ die höchste in $\mathfrak{a}$ aufgehende Potenz eines Primideals $\mathfrak{p}$, so ist me der Exponent der höchsten in η aufgehenden Potenz von $\mathfrak{p}$; hieraus folgt leicht, dass umgekehrt jede durch $\sqrt[m]{\eta}$ theilbare Zahl α in $\mathfrak{o}$ dem Ideale $\mathfrak{a}$ angehört; denn da

α^m theilbar durch η ist, so ist, wenn $\mathfrak{p}^a$ die höchste in α aufgehende Potenz von $\mathfrak{p}$ bedeutet, $ma \geqq me$, also $a \geqq e$, mithin geht $\mathfrak{p}^e$ auch in α auf (§. 163, 5.). *Das Ideal* $\mathfrak{a}$ *besteht daher aus allen durch* $\sqrt[m]{\eta}$ *theilbaren Zahlen in* $\mathfrak{o}$.

Eine unmittelbare Folgerung aus dem Vorhergehenden ist der wichtige Satz: *Je zwei ganze Zahlen* μ, ν *besitzen einen grössten gemeinschaftlichen Divisor* δ *der Art, dass die Quotienten* $\mu : \delta$, $\nu : \delta$ *relative Primzahlen werden.* Denn bildet man in irgend einem Körper Ω, welchem die beiden Zahlen μ, ν angehören, den grössten gemeinschaftlichen Theiler $\mathfrak{a}$ der beiden Hauptideale $\mathfrak{i}(\mu)$, $\mathfrak{i}(\nu)$, so wird, wenn $\mathfrak{a}^m = \mathfrak{i}(\eta)$ ist, $\sqrt[m]{\eta} = \delta$ ein solcher grösster gemeinschaftlicher Divisor von μ, ν; natürlich giebt es unendlich viele solche Zahlen δ, welche aber nicht wesentlich verschieden sind (§. 160, 6.).

Auf die weitere Entwicklung unserer Theorie der Ideale, wie z. B. auf die Untersuchung des Zusammenhangs zwischen den Idealen zweier verschiedenen Körper müssen wir hier verzichten.

§. 165.

Die Theorie der Ideale eines Körpers Ω hängt unmittelbar zusammen mit der Theorie der *zerlegbaren Formen*, welche demselben Körper entsprechen; wir beschränken uns hier darauf, diesen Zusammenhang in seinen Grundzügen anzudeuten.

1. Ist F ein Product aus n homogenen linearen Functionen $f_1, f_2 \ldots f_n$ von n Variabeln $h_1, h_2 \ldots h_n$, so wollen wir das Determinantenquadrat

$$\left(\Sigma \pm \frac{\partial f_1}{\partial h_1} \frac{\partial f_2}{\partial h_2} \cdots \frac{\partial f_n}{\partial h_n}\right)^2 = \Delta(F)$$

setzen und die *Determinante* der homogenen zerlegbaren Function F nennen*). Aus

$$\frac{\partial^2 \log F}{\partial h_r \partial h_s} = -\Sigma \frac{\partial \log f_t}{\partial h_r} \frac{\partial \log f_t}{\partial h_s}$$

folgt die Gleichung

$$F^2 \Sigma \pm \frac{\partial^2 \log F}{\partial h_1^2} \cdots \frac{\partial^2 \log F}{\partial h_n^2} = (-1)^n \Delta(F),$$

*) Für quadratische Formen ist diese Determinante das Vierfache von der in §. 53 definirten Determinante.

welcher man verschiedene andere Formen, z. B. auch die folgende

$$\begin{vmatrix} F & \frac{\partial F}{\partial h_1} & \cdots & \frac{\partial F}{\partial h_n} \\ \frac{\partial F}{\partial h_1} & \frac{\partial^2 F}{\partial h_1^2} & \cdots & \frac{\partial^2 F}{\partial h_1 \partial h_n} \\ \cdots & \cdots & \cdots & \cdots \\ \frac{\partial F}{\partial h_n} & \frac{\partial^2 F}{\partial h_n \partial h_1} & \cdots & \frac{\partial^2 F}{\partial h_n^2} \end{vmatrix} = (-1)^n F^{n-1} \Delta(F)$$

geben kann. Besitzt F lauter ganze rationale Coefficienten, so wollen wir ihren grössten gemeinschaftlichen Theiler t auch den *Theiler der Form F* nennen (vergl. §. 61); da sich nun leicht allgemein zeigen lässt, dass der Theiler eines Productes aus beliebigen Formen mit ganzen rationalen Coefficienten gleich dem Producte aus den Theilern der einzelnen Formen ist*), so folgt aus der vorstehenden Gleichung, dass $\Delta(F)$ eine ganze rationale, durch t^2 theilbare Zahl ist.

2. Aus der Definition eines Ideals $\mathfrak{a}$ (§. 163, 1.) ergiebt sich (zufolge §. 161), dass die sämmtlichen in ihm enthaltenen Zahlen α von der Form

$$\alpha = \sum x_\iota \alpha_\iota \tag{1}$$

sind, wo die Zahlen $\alpha_1, \alpha_2 \ldots \alpha_n$ particuläre Zahlen des Ideals $\mathfrak{a}$ bedeuten, während $x_1, x_2 \ldots x_n$ alle ganzen rationalen Zahlen durchlaufen dürfen. Bilden nun die Zahlen $\omega_1, \omega_2 \ldots \omega_n$ eine bestimmte Grundreihe des Körpers Ω (§. 162, 1.), so wollen wir die n Zahlen

$$\alpha_r = \sum a_\iota^{(r)} \omega_\iota, \tag{2}$$

welche eine Basis des Ideals $\mathfrak{a}$ bilden, in ihrer Aufeinanderfolge immer so wählen, dass ihre Coordinaten $a_\iota^{(r)}$ eine *positive* Determinante

$$a = \sum \pm a_1' a_2'' \ldots a_n^{(n)} = N(\mathfrak{a}) \tag{3}$$

besitzen; ferner ist die von der Wahl der Basis unabhängige Discriminante

$$\Delta(\alpha_1, \alpha_2 \ldots \alpha_n) = a^2 \Delta(\Omega). \tag{4}$$

Damit die Zahlen α wirklich ein Ideal bilden, ist erforderlich und hinreichend, dass die sämmtlichen Producte $\alpha_\iota \omega_{\iota'}$ wieder Zahlen in $\mathfrak{a}$ sind; es wird daher

*) Vergl. *Gauss: D. A.* art. 42.

$$\alpha\omega_r = \Sigma X_r^{(\iota)}\alpha_\iota = \Sigma X_r^{(\iota)} a_{\iota'}^{(\iota)} \omega_{\iota'}, \tag{5}$$

wo die n^2 Grössen $X_r^{(\iota)}$ homogene lineare Functionen der Veränderlichen $x_1, x_2 \ldots x_n$ mit ganzen rationalen Coefficienten bedeuten, und hieraus folgt

$$N(\alpha) = a\,X, \tag{6}$$

wo die Determinante

$$X = \Sigma \pm X_1' X_2'' \ldots X_n^{(n)} \tag{7}$$

eine homogene Form $n$ten Grades von $x_1, x_2 \ldots x_n$ bedeutet; ihre Coefficienten sind ganze rationale Zahlen, und man erkennt leicht, dass diese Form X irreductibel ist, weil sie durch die lineare Function α und folglich auch durch alle mit α conjugirten Functionen algebraisch theilbar ist (vergl. §. 159). Aus (4) und (6) folgt ihre Determinante

$$\Delta(X) = \Delta(\Omega). \tag{8}$$

Ist ferner k eine gegebene ganze rationale (von Null verschiedene) Zahl, so kann man den Variabeln x_ι stets solche ganze rationale Werthe beilegen, dass X relative Primzahl zu k wird. Man kann nämlich $\mathfrak{a}$ durch Multiplication mit einem Ideal $\mathfrak{m}$, welches ein relatives Primideal zu $\mathfrak{i}(k)$ ist, in ein Hauptideal $\mathfrak{i}(\alpha) = \mathfrak{a}\mathfrak{m}$ verwandeln (§. 163, 7.); ist nun $\mathfrak{p}$ irgend ein in $\mathfrak{m}$ aufgehendes Primideal, und p die durch $\mathfrak{p}$ theilbare rationale Primzahl (§. 163, 3.), so kann k nicht durch p theilbar sein, und da $N(\mathfrak{m})$ ein Product aus Potenzen solcher Primzahlen p ist (§. 163, 5.), so ist $N(\mathfrak{m})$ relative Primzahl zu k. Nun ist α in $\mathfrak{a}$ enthalten, also von der Form (1), wo die Grössen x_ι bestimmte ganze rationale Werthe haben, und $N(\alpha) = a\,X$; da andererseits $\mathfrak{i}(\alpha) = \mathfrak{a}\mathfrak{m}$, also $N(\alpha) = \pm a N(\mathfrak{m})$ ist (§. 163, 6.), so ergiebt sich, dass $X = \pm N(\mathfrak{m})$ relative Primzahl zu k ist, was zu beweisen war (vergl. §. 93). Hieraus folgt von selbst, dass X eine *ursprüngliche* Form ist, d. h. dass ihre Coefficienten keinen gemeinschaftlichen Theiler haben.

Wenn in dem Körper Ω keine Einheit existirt, deren Norm $= -1$ ist, so wollen wir ein Hauptideal $\mathfrak{i}(\eta)$ nur dann in die Hauptclasse E aufnehmen, wenn $N(\eta)$ positiv ist; ebenso sollen zwei Ideale $\mathfrak{a}$, $\mathfrak{a}'$ nur dann äquivalent heissen und in dieselbe Classe aufgenommen werden, wenn beide durch Multiplication mit demselben Ideale $\mathfrak{m}$ in Ideale der Hauptclasse E verwandelt werden (vergl. §. 164. Anm.). Gehört nun das Ideal $\mathfrak{a}$ der Classe A an, so leuchtet ein, dass jeder positive Werth der Form X, welcher

ganzen rationalen Werthen x_ι entspricht, die Norm eines zur entgegengesetzten Classe A^{-1} gehörenden Ideals $\mathfrak{m}$ ist, und dass umgekehrt die Norm eines jeden solchen Ideals $\mathfrak{m}$ durch die Form X *dargestellt* werden kann.

Wählt man statt der Basiszahlen $\alpha_1, \alpha_2 \ldots \alpha_n$ des Ideals andere $\beta_1, \beta_2 \ldots \beta_n$, welche aber ebenfalls der Bedingung genügen, dass die aus ihren Coordinaten gebildete Determinante *positiv* ist, so ist

$$\beta_r = \Sigma c_{r,\iota}\alpha_\iota, \quad \Sigma \pm c_{1,1}c_{2,2}\ldots c_{n,n} = +1, \tag{9}$$

und die der Basis $\alpha_1, \alpha_2 \ldots \alpha_n$ *entsprechende* Form X geht durch die Substitution

$$x_r = \Sigma c_{\iota,r}y_\iota, \tag{10}$$

deren Coefficienten $c_{\iota,r}$ ganze rationale Zahlen sind, in eine *äquivalente* Form Y über, welche der neuen Basis entspricht. Umgekehrt: ist Y eine mit X äquivalente Form, d. h. geht X durch eine ganzzahlige Substitution (10), deren Determinante $= +1$ ist, in Y über, so giebt es offenbar eine Basis des Ideals $\mathfrak{a}$, welcher diese Form Y entspricht. Allen Basen desselben Ideals $\mathfrak{a}$ entspricht daher eine bestimmte *Formenclasse*, d. h. ein System von Formen $X, Y \ldots$, der Art, dass je zwei von ihnen einander äquivalent sind, und wir wollen sagen, dass diese Formenclasse dem Ideale $\mathfrak{a}$ entspricht. Ist ferner η eine ganze Zahl von positiver Norm, so bilden die n Producte $\eta\alpha_\iota$ eine Basis des Ideals $\mathfrak{a}i(\eta)$, und hieraus folgt unmittelbar, dass allen mit $\mathfrak{a}$ äquivalenten Idealen, also einer ganzen Idealclasse, auch dieselbe Formenclasse entspricht. Auf die Frage, wie vielen Idealclassen eine und dieselbe Formenclasse entspricht, gehen wir hier nicht ein.

3. Bilden die Zahlen $\alpha_1, \alpha_2 \ldots \alpha_n$ die Basis eines Ideals $\mathfrak{a}$, ebenso die Zahlen $\beta_1, \beta_2 \ldots \beta_n$ die Basis eines Ideals $\mathfrak{b}$, so hängen die Basiszahlen $\gamma_1, \gamma_2 \ldots \gamma_n$ des Productes $\mathfrak{c} = \mathfrak{a}\mathfrak{b}$ mit denen der Ideale $\mathfrak{a}, \mathfrak{b}$ durch Gleichungen von der Form

$$\alpha_r\beta_s = \Sigma p_\iota^{r,s}\gamma_\iota, \quad \gamma_r = \Sigma q_{\iota,\varkappa}^{r}\alpha_\iota\beta_\varkappa \tag{11}$$

zusammen, wo die sämmtlichen $2n^3$ Grössen p und q ganze rationale Zahlen bedeuten; durch Substitution erhält man

$$\Sigma p_\iota^{r,s}q_\varkappa^{\iota,\varkappa} = 1 \quad \text{oder} \quad = 0, \tag{12}$$

je nachdem $r = s$ ist oder nicht. Bezeichnet man mit P alle aus den Zahlen p gebildeten Determinanten $n$ten Grades, mit Q die ent-

sprechenden Determinanten aus den Zahlen q, so folgt hieraus nach einem bekannten Satze

$$\Sigma PQ = 1; \tag{13}$$

also haben die Determinanten P keinen gemeinschaftlichen Theiler. Führt man nun drei Systeme von je n Variabeln x, y, z ein, und setzt

$$\alpha = \Sigma x_\iota \alpha_\iota, \quad \beta = \Sigma y_\iota \beta_\iota, \quad \gamma = \Sigma z_\iota \gamma_\iota, \tag{14}$$

so wird

$$N(\alpha) = aX, \quad N(\beta) = bY, \quad N(\gamma) = cZ, \tag{15}$$

wo X, Y, Z die zu $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ gehörigen Formen bedeuten, und

$$a = N(\mathfrak{a}), \quad b = N(\mathfrak{b}), \quad c = N(\mathfrak{c}) = ab \tag{16}$$

ist. Zwischen diesen Formen findet nun folgender Zusammenhang Statt. Setzt man

$$\alpha\beta = \gamma, \tag{17}$$

so werden die Variabeln z bilineare Functionen von den Variabeln x und y, nämlich

$$z_\tau = \Sigma p_\tau^{\iota,\iota'} x_\iota y_{\iota'}, \tag{18}$$

und da gleichzeitig $N(\alpha)N(\beta) = N(\gamma)$, d. h.

$$XY = Z \tag{19}$$

wird, so geht die Form Z durch diese bilineare Substitution in das Product der beiden Formen X, Y über, und wir wollen sagen, die Form Z sei aus den beiden Formen X, Y *zusammengesetzt*. Zwischen diesen Formen und der bilinearen Substitution findet nun ein einfacher Zusammenhang Statt; da nämlich

$$\alpha\beta_\tau = \Sigma \frac{\partial z_\iota}{\partial y_\tau}\gamma_\iota, \quad \beta\alpha_\tau = \Sigma \frac{\partial z_\iota}{\partial x_\tau}\gamma_\iota \tag{20}$$

ist, so erhält man, wenn man τ die Werthe $1, 2 \ldots n$ durchlaufen lässt, für $\mathfrak{Q}$ die n mit $\mathfrak{Q}$ conjugirten Körper setzt und die Determinanten nimmt,

$$X = \Sigma \pm \frac{\partial z_1}{\partial y_1} \cdots \frac{\partial z_n}{\partial y_n}, \quad Y = \Sigma \pm \frac{\partial z_1}{\partial x_1} \cdots \frac{\partial z_n}{\partial x_n}; \tag{21}$$

die Formen X, Y sind daher durch die Substitution (18) völlig bestimmt. Bezeichnet man ferner mit

$$\alpha' = \Sigma x'_\iota \alpha_\iota \tag{22}$$

die zu α adjungirte Function (§. 159, (8) und (38)), so ist

$$N(\alpha) = aX = \alpha\alpha', \tag{23}$$

und die n Grössen x' sind homogene Functionen $(n-1)$ten Grades von den Variabeln x mit rationalen Coefficienten. Durch Multiplication mit β ergiebt sich

$$a X \Sigma y_\iota \beta_\iota = \gamma \alpha'; \tag{24}$$

mithin sind die n Grössen

$$v_\iota = X y_\iota \tag{25}$$

bilineare Functionen von den Variabeln x', z mit rationalen Coefficienten; da ferner

$$a \Sigma \frac{\partial v_\iota}{\partial x_r'} \beta_\iota = \gamma \alpha_r, \tag{26}$$

so ergiebt sich, wie oben,

$$Z = a^{n-2} \Sigma \pm \frac{\partial v_1}{\partial x_1'} \cdots \frac{\partial v_n}{\partial x_n'}. \tag{27}$$

Hieraus folgt, dass auch die Form Z durch die bilineare Substitution (18) vollständig bestimmt ist; denn bezeichnet man mit $u_\iota^{(r)}$ den Coefficienten des Elementes

$$\frac{\partial z_\iota}{\partial y_r} \text{ in } \Sigma \pm \frac{\partial z_1}{\partial y_1} \cdots \frac{\partial z_n}{\partial y_n},$$

so ist auch

$$v_r = \Sigma u_\iota^{(r)} z_\iota, \tag{28}$$

und die n^2 Grössen $u_\iota^{(r)}$, welche homogene Functionen $(n-1)$ten Grades der Variabeln x mit ganzen rationalen Coefficienten sind, lassen sich folglich als homogene *lineare* Functionen der n Grössen x' darstellen. Statt der letzteren kann man auch n solche lineare Functionen von den n^2 Grössen $u_\iota^{(r)}$ mit ganzen rationalen Coefficienten einführen, durch welche sich umgekehrt auch die n^2 Grössen $u_\iota^{(r)}$ als lineare Functionen mit ganzen rationalen Coefficienten darstellen lassen. Auf die nähere Untersuchung dieser Eigenschaften der hier auftretenden bilinearen Substitutionen können wir aber nicht mehr eingehen.

4. Die ursprünglichen Formen X, welche den sämmtlichen Idealen des Körpers Ω entsprechen und alle dieselbe Determinante $\Delta(\Omega)$ besitzen, bilden nur einen speciellen Fall der Formen H, welche jeder beliebigen Basis $\omega_1, \omega_2 \ldots \omega_n$ des Körpers Ω entsprechen (§. 159). Für die Untersuchung dieser Formen ist es zweckmässig, den Begriff eines Ideals so zu erweitern, dass darunter ein System $\mathfrak{a}$ von ganzen Zahlen α des Körpers Ω verstanden wird, welche sich durch Addition, Subtraction und Multiplication reproduciren, mit der ferneren Bedingung, dass dieses System n unabhängige Zahlen enthält, oder dass, was dasselbe sagt, jede Zahl des Körpers durch Multiplication mit einer rationalen, von Null ver-

schiedenen Zahl in eine Zahl α des Systems $\mathfrak{a}$ verwandelt werden kann. Congruenzen in Bezug auf ein solches Ideal $\mathfrak{a}$ als Modul können addirt, subtrahirt und mit beliebigen Zahlen des Ideals multiplicirt werden. Von besonderer Wichtigkeit ist aber das System *aller* Zahlen, mit welchen solche Congruenzen multiplicirt werden dürfen, d. h. aller Zahlen, welche durch Multiplication mit allen Zahlen des Ideals $\mathfrak{a}$ in Zahlen desselben Ideals $\mathfrak{a}$ verwandelt werden; man erkennt sofort, dass dies System selbst ein Ideal ist, welches die Zahl 1 enthält. Dieses Ideal kann die *Ordnung von* $\mathfrak{a}$ oder auch ein *Einheitsideal* genannt werden, weil für die in ihm enthaltenen Zahlen die von *Dirichlet**) aufgestellte Theorie der Einheiten gilt, und wir wollen uns im Folgenden auf die Darstellung dieser Dirichlet'schen Principien beschränken, indem wir auf die weitere Entwicklung der allgemeinen Theorie der Ideale verzichten.

§. 166.

Wir nehmen im Folgenden an, dass die Basiszahlen $\omega_1, \omega_2 \ldots \omega_n$ des Körpers Ω zugleich die Basiszahlen einer *Ordnung* $\mathfrak{o}$ sind, d. h. dass die Zahl 1 und alle Producte $\omega_i \omega_{i'}$ *ganze* Coordinaten haben, woraus schon folgt, dass die Basiszahlen selbst ganze Zahlen sind. Die Zahlen in $\mathfrak{o}$, d. h. alle Zahlen $\omega = \sum h_i \omega_i$, deren Coordinaten h ganze rationale Zahlen sind, haben nun folgende Eigenschaften.

1. *Ist ω eine Zahl in $\mathfrak{o}$, so ist auch die zu ihr adjungirte Zahl ω' in $\mathfrak{o}$ enthalten.*

Da nämlich ω einer Gleichung $n$ten Grades mit ganzen rationalen Coefficienten genügt, deren letzter $= N(\omega) = \omega\omega'$ ist, so erhält man durch Division mit ω eine Gleichung von der Form

$$\omega' = c + c_1\omega + c_2\omega^2 + \cdots,$$

wo $c, c_1, c_2 \ldots$ ganze rationale Zahlen bedeuten; mithin ist ω' in $\mathfrak{o}$ enthalten.

2. Den mit Ω conjugirten n Körpern entsprechen ebensoviele homogene lineare Functionen ω der Coordinaten h, und ihr Product $N(\omega)$ wird, wenn die Coordinaten ganze Zahlen sind, ebenfalls

*) Vergl. §. 141, Anm.

eine ganze rationale Zahl und folglich absolut $\geqq 1$, ausgenommen, wenn alle Coordinaten verschwinden. Die n mit Ω conjugirten Körper enthalten entweder nur reelle Zahlen, oder es treten auch Paare von zwei solchen Körpern auf, dass wenn der eine die imaginäre Zahl $x + yi$ enthält, die conjugirte Zahl $x - yi$ sich in dem andern vorfindet. Wir wollen die Anzahl dieser imaginären Paare mit $n - \nu$, also die Anzahl der reellen Körper mit $2\nu - n$ bezeichnen; dann ist ν die Gesammtanzahl aller reellen Körper und imaginären Paare. Die einem imaginären Paare entsprechenden beiden Functionen ω sind von der Form $u + vi$ und $u - vi$, wo u und v zwei homogene lineare Functionen der Coordinaten bedeuten. Diese $2(n - \nu)$ Functionen u, v und die den reellen Körpern entsprechenden $(2\nu - n)$ Functionen ω bilden ein System von n reellen Functionen, die wir gemeinschaftlich mit w bezeichnen wollen, und deren Functionaldeterminante

$$= (2i)^{\nu - n} \sqrt{\Delta(\omega_1, \omega_2 \ldots \omega_n)},$$

also von Null verschieden ist, weil die Zahlen $\omega_1, \omega_2 \ldots \omega_n$ von einander unabhängig sind. Die Variabeln h sind daher umgekehrt völlig bestimmte lineare Functionen von den Grössen w; durchlaufen nun die letzteren stetig alle reellen Werthe, welche absolut kleiner als eine gegebene Constante sind, so bleiben auch die absoluten Werthe der Grössen h kleiner als eine entsprechende Constante und folglich wird auf diese Weise nur eine endliche Anzahl von Zahlen der Ordnung $\mathfrak{o}$ erzeugt, vielleicht gar keine.

Verstehen wir, wie üblich, unter dem Modulus $M(z)$ einer complexen Grösse $z = x + yi$ die positive Quadratwurzel aus $(x^2 + y^2)$, so können wir dies Resultat auch so aussprechen: *Es giebt in* $\mathfrak{o}$ *nur eine endliche Anzahl von Zahlen* ω *der Art, dass die Moduln aller mit* ω *conjugirten Zahlen, also auch die absoluten Werthe der Grössen* w *kleiner als eine vorgeschriebene Constante ausfallen.*

3. Wir theilen nun die n Körper, also auch die n Functionen ω nach Belieben in zwei Reihen, doch so, dass jede dieser Reihen wenigstens eine Function enthält, und dass je zwei Functionen $u \pm vi$ eines imaginären Paares in eine und dieselbe Reihe fallen (also ist der Fall $n = 1$ auszunehmen, ebenso der Fall $n = 2$ bei negativer Grundzahl). Bedeutet ferner c den grössten Werth, welchen die Modulsumme $\Sigma M(\omega_s)$ in irgend einer der n Functionen ω erreicht, so gilt folgender Satz:

Ist a ein beliebig kleiner, b ein beliebig grosser positiver gegebener Werth, so giebt es in $\mathfrak{o}$ eine solche Zahl ω, dass $M(\omega)$ in der ersten Reihe $< a$, in der zweiten $> b$, und dass $N(\omega)$ absolut $< (3c)^n$ wird.

Ist k eine bestimmte positive ganze rationale Zahl, und legt man jeder Coordinate h einen der $(k+1)$ Werthe $0, 1, 2 \ldots k$ bei, so wird durchweg $M(\omega) \leqq ck$, und die n Werthe w liegen zwischen den Grenzen $\pm ck$. Wir betrachten nun zunächst die der *ersten* Reihe angehörigen r Functionen ω oder w; da $n > r > 0$, und $k > 0$ ist, so ist auch

$$(k+1)^{\frac{n}{r}} > k^{\frac{n}{r}} + 1,$$

und folglich kann man eine positive ganze rationale Zahl m so wählen, dass

$$(k+1)^n > m^r > k^n$$

wird; setzt man nun zur Abkürzung

$$d = \frac{2ck}{m} < 2ck^{1-\frac{n}{r}},$$

so wird das Gebiet aller zwischen den Grenzen $\pm ck$ liegenden reellen Werthe durch Einschaltung der $(m-1)$ Zahlen

$$-ck+d, \quad -ck+2d \ldots -ck+(m-1)d$$

in m Intervalle von gleicher Grösse d getheilt, wobei man diese $(m-1)$ Zahlen selbst nach Belieben dem einen oder anderen der beiden benachbarten Intervalle zurechnen kann. Da nun jeder der r Werthe w aus der ersten Reihe einem und nur einem dieser m Intervalle angehört, so ist m^r die Anzahl der verschiedenen denkbaren Fälle, welche die Vertheilung der r Werthe w auf diese m Intervalle darbieten kann. Da ferner, wenn jede der n Coordinaten h alle $(k+1)$ Werthe $0, 1, 2 \ldots k$ durchläuft, $(k+1)^n$ solche Systeme von r zusammengehörigen Werthen w entstehen, so müssen, weil $(k+1)^n > m^r$ ist, mindestens zwei *verschiedene* solche Werthsysteme hinsichtlich ihrer Vertheilung auf die m Intervalle vollständig übereinstimmen, in der Art, dass je zwei Werthe w', w'', welche eine und dieselbe Function w in diesen beiden Systemen annimmt, auch einem und demselben Intervall angehören. Wird nun das System der r Werthe w' durch die Coordinaten h_i', ferner das System der r Werthe w'' durch die Coordinaten h_i'' hervorgebracht, so entspricht den Coordinaten $h_i = h_i' - h_i''$ ein System von

r Werthen $w = w' - w''$, welche absolut den Werth d nicht übersteigen. Für diese ganzen Coordinaten h_ι, welche absolut $\leqq k$ sind und nicht sämmtlich verschwinden, wird daher in der *ersten* Reihe

$$M(\omega) \leqq d\sqrt{2} < 3ck^{1-\frac{n}{r}}.$$

Ist ferner P das Product aus den r Werthen ω der ersten Reihe, und $N(\omega) = PQ$, so ergiebt sich $M(P) < (3c)^r k^{r-n}$, $M(Q) \leqq (ck)^{n-r}$, mithin absolut

$$N(\omega) < (3c)^n.$$

Da endlich $N(\omega)$ eine von Null verschiedene ganze rationale Zahl ist, so wird $M(PQ) = M(P)M(Q) \geqq 1$, also $M(Q) > (3c)^{-r}k^{n-r}$; ist nun ω eine der $(n-r)$ Functionen der zweiten Reihe, und $Q = \omega\theta$, so ist $M(\theta) \leqq (ck)^{n-r-1}$, und folglich wird in der *zweiten* Reihe

$$M(\omega) > (3c)^{1-n}k.$$

Offenbar kann nun, wie klein auch a, und wie gross auch b sein mag, k stets so gross gewählt werden, dass $M(\omega)$ in der ersten Reihe $< a$, in der zweiten $> b$ ausfällt, während $N(\omega)$ absolut $< (3c)^n$ wird; was zu beweisen war.

4. Aus dem soeben bewiesenen Satze ergiebt sich, indem man dieselbe Eintheilung in zwei Reihen beibehält, dass man eine nie abreissende Kette von aufeinander folgenden, von Null verschiedenen Zahlen ω in $\mathfrak{o}$ aufstellen kann, deren Normen $< (3c)^n$ sind, und welche ausserdem noch die zweite Eigenschaft besitzen, dass $M(\omega)$ in der ersten Reihe kleiner, in der zweiten grösser ausfällt, als die Moduln aller *vorhergehenden* Zahlen ω und der mit ihnen conjugirten Zahlen; denn bezeichnet man mit a den kleinsten, mit b den grössten unter allen Moduln der schon gebildeten Zahlen ω und der mit ihnen conjugirten Zahlen, so giebt es zufolge des bewiesenen Satzes immer noch eine Zahl ω der Art, dass $M(\omega)$ in der ersten Reihe $< a$, in der zweiten $> b$ ausfällt, während $N(\omega)$ absolut genommen ebenfalls $< (3c)^n$ wird; diese neue Zahl ω ist daher auch von Null und von allen vorhergehenden Zahlen ω verschieden. Wir theilen nun die Zahlen ω dieser Kette in Gruppen ein, indem wir zwei von ihnen stets und nur dann in dieselbe Gruppe aufnehmen, wenn sie dieselbe Norm m besitzen, und wenn ausserdem die Coordinaten ihrer Differenz sämmtlich durch m theilbar sind; da nun die hier auftretenden Normen m ganze rationale Zahlen

und absolut $< (3c)^n$ sind, und da die Coordinaten einer Zahl ω hinsichtlich ihrer Reste (mod. m) höchstens $(\pm m)^n$ verschiedene Fälle darbieten können, so kann in dieser Kette von Zahlen ω auch nur eine *endliche* Anzahl verschiedener Gruppen auftreten, und folglich muss bei hinreichender Fortsetzung der nie abbrechenden Kette eine Zahl β in ihr erscheinen, welche mit einer früheren Zahl α in dieselbe Gruppe fällt. Dann ist also $N(\alpha) = N(\beta) = \beta\beta' = m$, und $\alpha = \beta + m\gamma = \beta(1 + \gamma\beta') = \beta\varepsilon$, wo β' (zufolge 1.) und γ, folglich auch $\varepsilon = 1 + \gamma\beta'$ Zahlen in $\mathfrak{o}$ bedeuten; zugleich ergiebt sich, da $N(\alpha) = N(\beta) = N(\beta\varepsilon)$ von Null verschieden ist, $N(\varepsilon) = 1$, und aus $M(\alpha) = M(\beta)M(\varepsilon)$ folgt, dass $M(\varepsilon)$ in der ersten Reihe > 1, in der zweiten < 1 ist. Versteht man unter einer *Einheit* im Folgenden stets eine Zahl in $\mathfrak{o}$, deren Norm $= +1$ ist, so haben wir daher folgendes Resultat gewonnen:

Es giebt eine Einheit von der Art, dass die Moduln der mit ihr conjugirten Zahlen in der ersten Reihe > 1, *in der zweiten* < 1 *sind.*

5. Multiplicirt man je zwei zusammengehörige imaginäre Functionen $\omega = u \pm vi$ mit einander, so bilden diese $(n - \nu)$ Producte $(u^2 + v^2)$ und die $(2\nu - n)$ reellen Functionen ω ein System von ν reellen, theils quadratischen, theils linearen Functionen f', $f'' \ldots f^{(\nu)}$ der Coordinaten; nennt man die *reellen* Bestandtheile ihrer Logarithmen kurz die (conjugirten) *Logarithmen von* ω, so kann man das eben erhaltene Resultat auch so aussprechen:

Theilt man die ν *Functionen* f *nach Belieben in zwei Reihen, doch so, dass jede dieser Reihen wenigstens eine Function enthält, so existirt stets eine Einheit* ε, *deren Logarithmen* $e', e'' \ldots e^{(\nu)}$ *positiv oder negativ sind, je nachdem sie der ersten oder der zweiten Reihe entsprechen.*

Da die Summe der Logarithmen einer Zahl ω gleich dem reellen Bestandtheile des Logarithmen von $N(\omega)$ ist, so ist die Summe der Logarithmen $e', e'' \ldots e^{(\nu)}$ einer Einheit ε stets $= 0$; hat man daher ν beliebige Einheiten $\varepsilon_1, \varepsilon_2 \ldots \varepsilon_\nu$, so ist die aus den zugehörigen ν^2 Logarithmen gebildete Determinante

$$\Sigma \pm e_1' e_2'' \ldots e_\nu^{(\nu)} = 0;$$

lässt man aber einen dieser Logarithmen, z. B. den letzten $e^{(\nu)}$, welcher der Function $f^{(\nu)}$ entspricht, stets weg, so gilt folgender Fundamentalsatz:

Es giebt immer ein System S von $(\nu-1)$ unabhängigen, d. h. solchen Einheiten $\varepsilon_1, \varepsilon_2 \ldots \varepsilon_{\nu-1}$, dass die aus ihren Logarithmen gebildete Determinante

$$L = \Sigma \pm e_1' e_2'' \ldots e_{\nu-1}^{(\nu-1)}$$

einen positiven, also von Null verschiedenen Werth besitzt.

Ist nämlich $\nu = 2$, so folgt aus dem obigen Satze, wenn man f' in die erste, f'' in die zweite Reihe aufnimmt, die Existenz einer Einheit ε, für welche der Logarithme e' positiv ausfällt (hiermit ist für den nicht ausgeschlossenen Fall $n = 2$ die Theorie der Einheiten im Wesentlichen absolvirt; vergl. §. 142). Ist aber $\nu > 2$ und $m < \nu$, und hat man schon $m-1$ Einheiten $\varepsilon_1, \varepsilon_2 \ldots \varepsilon_{m-1}$ aufgestellt, für welche die Determinante

$$\Sigma \pm e_1' e_2'' \ldots e_{m-1}^{(m-1)}$$

einen positiven Werth $E^{(m)}$ hat, so kann man mit Hülfe desselben Satzes die Existenz einer Einheit ε_m beweisen, für welche auch die Determinante

$$\Sigma \pm e_1' e_2'' \ldots e_{m-1}^{(m-1)} e_m^{(m)}$$

positiv ausfällt; ordnet man dieselbe nach den Logarithmen e_m', $e_m'' \ldots e_m^{(m)}$ der neuen Einheit ε_m, so nimmt sie die Form

$$E' e_m' + E'' e_m'' + \cdots + E^{(m-1)} e_m^{(m-1)} + E^{(m)} e_m^{(m)}$$

an, wo $E^{(m)}$ der Annahme zufolge positiv ist, während die übrigen aus den Logarithmen von $\varepsilon_1, \varepsilon_2 \ldots \varepsilon_{m-1}$ gebildeten Determinanten $E', E'' \ldots E^{(m-1)}$ positiv, negativ oder auch $= 0$ sein können. Nimmt man nun von den Functionen $f', f'' \ldots f^{(m)}$ alle diejenigen in die erste Reihe auf, denen positive Werthe $E', E'' \ldots E^{(m)}$ entsprechen, also jedenfalls die Function $f^{(m)}$, während die übrigen und die Functionen $f^{(m+1)} \ldots f^{(\nu)}$, also jedenfalls $f^{(\nu)}$ in die zweite Reihe fallen, so existirt zufolge des obigen Satzes eine Einheit ε_m, deren Logarithmen $e_m', e_m'' \ldots e_m^{(\nu)}$ positiv oder negativ ausfallen, je nachdem sie der ersten oder zweiten Reihe entsprechen; mithin enthält das obige Aggregat mindestens ein positives Glied $E^{(m)} e_m^{(m)}$, und die übrigen Glieder sind nicht negativ, so dass das Aggregat selbst einen positiven Werth erhält, was zu beweisen war. Auf diese Weise kann man offenbar von $m = 2$ bis $m = \nu - 1$ fortschliessen, und erhält zuletzt das in dem Satze ausgesprochene Resultat.

6. Behält man die bisherigen Bezeichnungen bei, und lässt man $m_1, m_2 \ldots m_{\nu-1}$ alle ganzen rationalen Zahlen von $-\infty$ bis $+\infty$ durchlaufen, so bilden die entsprechenden Zahlen

$$\eta = \varepsilon_1^{m_1} \varepsilon_2^{m_2} \ldots \varepsilon_{\nu-1}^{m_{\nu-1}}$$

eine Gruppe (S) von unendlich vielen Einheiten, welche sich durch Multiplication und Division reproduciren.

Es fragt sich nun, ob ausser diesen Einheiten η noch andere existiren. Ist ε eine beliebige Einheit, deren Logarithmen $e', e'' \ldots e^{(\nu)}$ sind, so giebt es, weil die Determinante L von Null verschieden ist, stets ein und nur ein System reeller Grössen $x_1, x_2 \ldots x_{\nu-1}$, welche den ν Gleichungen

$$\begin{aligned} e'_1 x_1 + e'_2 x_2 + \cdots + e'_{\nu-1} x_{\nu-1} &= e' \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots & \\ e_1^{(\nu)} x_1 + e_2^{(\nu)} x_2 + \cdots + e_{\nu-1}^{(\nu)} x_{\nu-1} &= e^{(\nu)} \end{aligned}$$

genügen, deren letzte eine Folge der übrigen ist; wir nennen diese Werthe $x_1, x_2 \ldots x_{\nu-1}$ kurz die *Exponenten* der Einheit ε in Bezug auf das System S der $(\nu - 1)$ unabhängigen Einheiten $\varepsilon_1, \varepsilon_2 \ldots \varepsilon_{\nu-1}$; die Exponenten eines Productes entstehen offenbar durch Addition der entsprechenden Exponenten der Factoren, und die Exponenten einer Einheit η aus der Gruppe (S) sind ganze rationale Zahlen $m_1, m_2 \ldots m_{\nu-1}$. Sind die Exponenten einer Einheit ε sämmtlich < 1 und nicht negativ, so soll ε eine in Bezug auf S *reducirte* Einheit heissen. Zunächst leuchtet ein, dass es nur eine *endliche* Anzahl solcher reducirten Einheiten giebt; lässt man nämlich in den vorstehenden linearen Ausdrücken linker Hand die Grössen $x_1, x_2 \ldots x_{\nu-1}$ alle reellen Werthe zwischen 0 und 1 durchlaufen, so bleiben die Werthe dieser linearen Ausdrücke absolut kleiner als eine von den Coefficienten, d. h. von dem System S abhängige endliche Constante; dasselbe gilt daher von den Logarithmen $e', e'' \ldots e^{(\nu)}$ einer reducirten Einheit ε, und folglich sind auch die Moduln aller mit ε conjugirten Zahlen kleiner als eine von S abhängige Constante, woraus (mit Rücksicht auf 2.) die Richtigkeit der obigen Behauptung sich unmittelbar ergiebt.

Jede beliebige Einheit ε lässt sich stets und nur auf einzige Art als ein Product aus einer reducirten Einheit ϱ und einer Einheit η aus der Gruppe (S) darstellen. Soll nämlich $\varepsilon = \varrho\eta$, also $\varepsilon\eta^{-1} = \varrho$ eine reducirte Einheit sein, so müssen, wenn $x_1, x_2 \ldots x_{\nu-1}$ die Exponenten von ε bedeuten, die Exponenten m_1,

$m_2 \ldots m_{\nu-1}$ der der Gruppe (S) angehörigen Einheit η solche ganze rationale Zahlen sein, dass die Exponenten von ϱ, also die Zahlen $x_1 - m_1$, $x_2 - m_2 \ldots x_{\nu-1} - m_{\nu-1}$ sämmtlich < 1 und nicht negativ werden; dies kann immer und nur dadurch erreicht werden, dass man für $m_1, m_2 \ldots m_{\nu-1}$ resp. die grössten in den reellen Werthen $x_1, x_2 \ldots x_{\nu-1}$ enthaltenen ganzen rationalen Zahlen wählt (vergl. §§. 43, 44); also ist η und folglich auch ϱ vollständig bestimmt.

Ist r die Anzahl aller von einander verschiedenen reducirten Einheiten ϱ (unter denen sich auch die Zahl 1 befindet), und ε irgend eine Einheit, so ist ε^r eine der Gruppe (S) angehörige Einheit; durchläuft nämlich ϱ alle reducirten Einheiten, so ist jedes der r Producte $\varepsilon\varrho$ von der Form $\sigma\eta$, wo σ eine reducirte Einheit, η eine Einheit aus der Gruppe (S) bedeutet, und σ muss ebenfalls alle r reducirten Einheiten durchlaufen, weil aus $\varepsilon\varrho = \sigma\eta$ und $\varepsilon\varrho' = \sigma\eta'$ auch die Gleichung $\varrho'\eta = \varrho\eta'$ folgen würde, welche, wie oben gezeigt ist, nur dann bestehen kann, wenn $\varrho = \varrho'$ ist; multiplicirt man nun die r Gleichungen von der Form $\varepsilon\varrho = \sigma\eta$, und dividirt durch das Product der r reducirten Einheiten ϱ oder σ, so folgt, dass ε^r ein Product aus r Einheiten der Gruppe (S), mithin selbst eine Einheit dieser Gruppe ist.

Die Exponenten von ε^r sind daher immer ganze rationale Zahlen $m_1, m_2 \ldots m_{\nu-1}$, und folglich sind die Exponenten einer jeden Einheit ε stets *rationale* Zahlen mit dem gemeinschaftlichen Nenner r. Sind nun $\delta_1, \delta_2 \ldots \delta_{\nu-1}$ beliebige Einheiten, deren Logarithmen mit d bezeichnet werden, so folgt, dass die ihnen entsprechende Determinante

$$= \Sigma \pm d_1' d_2'' \ldots d_{\nu-1}^{(\nu-1)} = \frac{mL}{r^{\nu-1}}$$

ist, wo m die aus den $(\nu-1)^2$ Exponenten der Einheiten δ_1^r, $\delta_2^r \ldots \delta_{\nu-1}^r$ gebildete Determinante, also eine *ganze* rationale Zahl bedeutet, welche von Null verschieden ist, wenn $\delta_1, \delta_2 \ldots \delta_{\nu-1}$ ebenfalls ein System von unabhängigen Einheiten bilden. Hieraus ergiebt sich die wichtige Folgerung, dass es unter allen Systemen von $(\nu-1)$ unabhängigen Einheiten ein solches geben muss, für welches die entsprechende Determinante absolut genommen einen *Minimalwerth* annimmt; denn unter allen hier auftretenden ganzen rationalen, von Null verschiedenen Zahlen m muss es eine absolut kleinste geben. Ein solches System von $(\nu-1)$ unabhängigen Einheiten soll ein *Fundamentalsystem* heissen.

7. Wir wollen nun annehmen, das obige System S der $(\nu-1)$ unabhängigen Einheiten sei ein solches Fundamentalsystem, also L der eben erwähnte Minimalwerth, so folgt zunächst, dass die Exponenten $x_1, x_2 \ldots x_{\nu-1}$ einer jeden in Bezug auf S reducirten Einheit ε sämmtlich $= 0$ sind; wäre nämlich z. B. x_1 von Null verschieden, also positiv und < 1, so wäre die den $(\nu-1)$ Einheiten $\varepsilon, \varepsilon_2 \ldots \varepsilon_{\nu-1}$ entsprechende Determinante

$$\Sigma \pm e' e_2'' \ldots e_{\nu-1}^{(\nu-1)} = L x_1$$

von Null verschieden und absolut kleiner als L, was mit unserer Annahme streitet. Da ferner die Exponenten eines Productes zweier Einheiten durch Addition der entsprechenden Exponenten der beiden Factoren entstehen, so sind die Exponenten eines jeden Productes $\varrho\varrho' = \varrho''$ aus zwei reducirten Einheiten ϱ, ϱ' sämmtlich $= 0$, d. h. ein solches Product ist wieder eine reducirte Einheit. Hieraus folgt unmittelbar, dass die sämmtlichen r reducirten Einheiten ϱ die Wurzeln der Gleichung $\varrho^r = 1$ sind; durchläuft nämlich ϱ' alle reducirten Einheiten, so gilt dasselbe von $\varrho'' = \varrho\varrho'$; multiplicirt man diese r Gleichungen, und dividirt durch das Product aller reducirten Einheiten ϱ' oder ϱ'', so folgt $\varrho^r = 1$. Da endlich schon (in 6.) gezeigt ist, dass jede Einheit ε von der Form $\varrho\eta$ ist, wo ϱ eine reducirte, und η eine Einheit aus der Gruppe (S) bedeutet, so haben wir hiermit den folgenden grossen Satz von *Dirichlet* bewiesen:

Bezeichnet ν die Gesammtanzahl der reellen und imaginären Paare unter den mit Ω conjugirten Körpern, so giebt es in jeder Ordnung $\mathfrak{o}$ immer $(\nu-1)$ Fundamentaleinheiten von solcher Beschaffenheit, dass, wenn man dieselben beliebig oft in einander multiplicirt und dividirt und dem so gebildeten allgemeinen Product gewisse besondere Einheiten ϱ in endlicher Anzahl einzeln als Factor zugesellt, alle Einheiten dieser Ordnung und zwar jede nur einmal dargestellt werden; ist r die Anzahl dieser besonderen Einheiten ϱ, so sind sie die Wurzeln der Gleichung $\varrho^r = 1$.

§. 167.

Der eben bewiesene Satz bildet neben der Theorie der Ideale (§. 163) die wichtigste Grundlage für das tiefere Studium der ganzen Zahlen des Körpers Ω, und er ist unentbehrlich für die wirkliche Bestimmung der Anzahl der Idealclassen nach Dirichlet'schen Principien. Diese geschieht dadurch, dass der Grenzwerth der über alle Ideale $\mathfrak{a}$ ausgedehnten Summe

$$\Sigma \frac{s-1}{N(\mathfrak{a})^s}$$

für unendlich kleine positive Werthe von $(s-1)$ auf doppelte Weise ermittelt wird. Einmal muss das System aller Idealnormen $N(\mathfrak{a})$ genau definirt werden, d. h. es muss von jeder positiven ganzen rationalen Zahl m festgestellt werden, wie gross die Anzahl $\tau(m)$ der verschiedenen Ideale $\mathfrak{a}$ ist, deren Norm $= m$; die Beantwortung dieser Frage fällt der Theorie der Ideale zu. Die Summe nimmt dann die Form

$$(s-1) \Sigma \frac{\tau(m)}{m^s}$$

an, wo m alle positiven ganzen rationalen Zahlen durchlaufen muss*).

Das andere Mal theilt man die obige Summe in Partialsummen ein, deren jede alle die Glieder enthält, welche den sämmtlichen Idealen $\mathfrak{a}$ einer und derselben Classe entsprechen, und es sind bei

*) Hierbei zeigt sich, dass $\tau(mm') = \tau(m)\tau(m')$ ist, wenn m, m' relative Primzahlen sind; mithin ist $\tau(m)$ vollständig bekannt, wenn für jede rationale Primzahl p die Zerlegung von $i(p)$ in Primideale bekannt ist; die Primzahlen p zerfallen hiernach in eine endliche Anzahl verschiedener Arten, in der Weise, dass für alle Primzahlen p gleicher Art die Bestimmung von $\tau(p^e)$ nach derselben Regel geschieht. Die obige Summe lässt sich daher gewissen Umformungen unterwerfen, welche für *alle* Körper gültig sind; am einfachsten gestalten sich dieselben für Galois'sche Körper.

der weiteren Untersuchung hauptsächlich folgende Momente zu berücksichtigen.

Nimmt man, falls in Ω keine Einheit von der Norm -1 existirt, ein Ideal $\mathfrak{i}(\omega)$ nur dann in die Hauptclasse E auf, wenn $H = N(\omega)$ *positiv* ist, so braucht man nur alle ganzen Zahlen ω von positiver Norm zu betrachten, und es wird, wenn α eine bestimmte solche Zahl bedeutet, $\mathfrak{i}(\omega)$ stets und nur dann mit $\mathfrak{i}(\alpha)$ identisch sein, wenn $\omega = \varepsilon\alpha$, und ε eine Einheit von positiver Norm ist. Abgesehen von dem Falle eines quadratischen imaginären Körpers wird daher jedes Ideal der Hauptclasse unendlich oft auftreten, und es kommt darauf an, ω solchen Bedingungen zu unterwerfen, dass jedes Ideal $\mathfrak{i}(\omega)$ nur einmal oder wenigstens nicht unendlich oft erscheint (vergl. §. 87). Behalten wir die Bezeichnungen des vorhergehenden Paragraphen bei, indem wir annehmen, dass die Ordnung $\mathfrak{o}$ alle ganzen Zahlen des Körpers umfasst, so kann dies in folgender Weise erreicht werden.

Dividirt man jede der ν Functionen $f', f'' \ldots f^{(\nu)}$, je nachdem sie linear oder quadratisch ist, durch $\sqrt[\nu]{H}$ oder durch $\sqrt[\nu]{H^2}$, und bezeichnet man mit $l', l'' \ldots l^{(\nu)}$ die reellen Bestandtheile der Logarithmen dieser ν Quotienten, so ist $l' + l'' + \cdots + l^{(\nu)} = 0$, und es giebt stets ein und nur ein System von reellen Grössen $x_1, x_2 \ldots x_{\nu-1}$, welche den Gleichungen

$$e_1' x_1 + e_2' x_2 + \cdots + e_{\nu-1}' x_{\nu-1} = l'$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$e_1^{(\nu)} x_1 + e_2^{(\nu)} x_2 + \cdots + e_{\nu-1}^{(\nu)} x_{\nu-1} = l^{(\nu)}$$

genügen; nennen wir sie kurz die *Exponenten von* ω (vergl. §. 166,6.), so leuchtet ein, dass die Exponenten eines Productes durch Addition der entsprechenden Exponenten der Factoren entstehen. Nennt man ferner ω eine *reducirte* Zahl, wenn ihre Exponenten sämmtlich < 1 und nicht negativ sind, und lässt man ε zunächst nur alle Einheiten η durchlaufen, welche der Gruppe (S) angehören, während α eine gegebene ganze Zahl bedeutet, so ergiebt sich, dass unter allen Producten $\omega = \eta\alpha$ eine und nur eine reducirte ganze Zahl, und folglich unter allen Producten $\omega = \varepsilon\alpha$ genau r reducirte ganze Zahlen ω existiren, wenn r wieder die Anzahl der in Bezug auf S reducirten Einheiten bedeutet. Mithin ist die auf die Hauptclasse E bezügliche Partialsumme gleich

$$\frac{s-1}{r} \sum \frac{1}{N(\omega)^s} = \frac{s-1}{r} \sum \frac{1}{H^s},$$

wo ω alle reducirten ganzen Zahlen durchlaufen muss, d. h. alle ganzen Zahlen $\omega = \sum h_\iota \omega_\iota$ von positiver Norm H, deren Exponenten den Bedingungen

$$0 \leqq x_1 < 1, \quad 0 \leqq x_2 < 1 \ldots 0 \leqq x_{\nu-1} < 1$$

genügen.

Zur Bestimmung des Grenzwerthes g dieser Partialsumme für unendlich kleine positive Werthe von $(s-1)$ dienen nun die von *Dirichlet* aufgestellten Principien. Bedeutet t eine über alle Grenzen wachsende positive Grösse, T die Anzahl der hier auftretenden Normen H, welche nicht grösser als t sind, und nähert sich der Quotient $T:t$ einem endlichen Grenzwerth k, so ist (§. 118)

$$g = \frac{k}{r}.$$

Um ferner den Grenzwerth k des Quotienten $T:t$ zu ermitteln, muss der von *Dirichlet* benutzte geometrische Satz (§. 120) zu dem folgenden Princip erhoben werden, welches seinen unmittelbaren Grund in dem Begriff eines vielfachen bestimmten Integrals findet: Durchlaufen die n *stetigen*, reellen Variabeln h_ι ein endliches Gebiet G von n Dimensionen, und bedeutet T', wenn δ eine beliebig kleine positive Grösse ist, die Anzahl derjenigen dem Gebiete G angehörigen Werthsysteme der Variabeln h_ι, für welche die n Quotienten $h_\iota : \delta$ *ganze rationale* Zahlen werden, so wird für unendlich kleine Werthe von δ

$$\lim (T' \delta^n) = \int dh_1 dh_2 \ldots dh_n,$$

wo das $n$fache Integral über das Gebiet G auszudehnen ist. Definirt man nun das Gebiet G durch die obigen Bedingungen für die Exponenten $x_1, x_2 \ldots x_{\nu-1}$ von $\omega = \sum h_\iota \omega_\iota$ und durch die Bedingung

$$0 < H \leqq 1,$$

und bedenkt, dass die Exponenten von ω nur von den *Verhältnissen* der Variabeln h_ι abhängen, während H eine homogene Function $n$ten Grades ist, so leuchtet unmittelbar ein, dass T' durchaus identisch mit T ist, sobald

$$\delta = \frac{1}{\sqrt[n]{t}}$$

genommen wird; denn wenn die ganzen rationalen Zahlen h_ι durch $h_\iota \sqrt[n]{t} = h_\iota : \delta$ ersetzt werden, so geht die durch T reducirte ganze

Zahlen ω erfüllte Bedingung $0 < H \leqq t$ in $0 < H \leqq 1$ über, während die Bedingungen für die Exponenten ungeändert bleiben. Da zugleich $T'\delta^n = T:t$ ist, so ergiebt sich also, dass der Grenzwerth der auf die Hauptclasse E bezüglichen Partialsumme

$$g = \frac{1}{r}\int dh_1\, dh_2 \ldots dh_n$$

ist.

Um den Werth dieses Integrals zu erhalten, führe man als neue unabhängige Variabele $H, x_1, x_2 \ldots x_{\nu-1}$ und die zwischen den Grenzen 0 und 2π liegenden Winkel $\varphi_1, \varphi_2 \ldots \varphi_{n-\nu}$ ein, welche den $(n-\nu)$ mit ω conjugirten imaginären Paaren $u \pm vi$ in der Weise entsprechen, dass

$$u + vi = \sqrt{f}.e^{\varphi i}, \quad f = u^2 + v^2$$

wird. Jedem System der ursprünglichen Variabeln h_ι entspricht ein und nur ein System der neuen Variabeln; umgekehrt aber entsprechen jedem System der neuen Variabeln, wenn H positiv genommen wird, $2^{2\nu-n-1}$ verschiedene Systeme der alten Variabeln h_ι; denn durch die Werthe von $H, x_1, x_2 \ldots x_{\nu-1}$ werden nur die absoluten Werthe der $(2\nu-n)$ reellen mit ω conjugirten Functionen bestimmt, und da ihr Product positiv sein muss, so kann man ihnen, mit Ausnahme einer, sowohl das positive wie das negative Vorzeichen geben; nur in dem Falle $n = 2\nu$, wenn gar kein reeller Körper mit Ω conjugirt ist, muss diese Anzahl $2^{2\nu-n-1}$ wieder durch 1 ersetzt werden. Geht man ferner von den ursprünglichen Variabeln h_ι successive zu den mit ω conjugirten oder den n Functionen w, von diesen zu $f', f'' \ldots f^{(\nu)}, \varphi_1, \varphi_2 \ldots \varphi_{n-\nu}$, von diesen zu den neuen Variabeln über, so findet man leicht, dass die entsprechende Functional-Determinante gleich

$$\frac{L}{i^{\nu-n}\sqrt{\Delta(\Omega)}} = \frac{\Sigma \pm e_1 e_2'' \ldots e_{\nu-1}^{(\nu-1)}}{i^{\nu-n}\sqrt{\Delta(\Omega)}}$$

ist; mithin ist der auf die Hauptclasse E bezügliche Grenzwerth g gleich

$$\frac{2^{\nu-1}\pi^{n-\nu}L}{r i^{\nu-n}\sqrt{\Delta(\Omega)}},$$

oder doppelt so gross, falls $n = 2\nu$ ist (wenn zugleich $n = 2$ ist, so ist $L = 1$ zu setzen, und r bedeutet die Anzahl aller Einheiten).

An dieses Resultat knüpfen wir zunächst folgende Bemerkung. Nimmt man in die erste Partialsumme nicht alle Ideale der Haupt-

classe E, sondern nur diejenigen Ideale $\mathfrak{e}$ auf, welche zugleich durch ein bestimmtes Ideal $\mathfrak{m}$ theilbar sind, so treten an die Stelle der Basiszahlen $\omega_1, \omega_2 \ldots \omega_n$ von $\mathfrak{o}$ die Basiszahlen $\mu_1, \mu_2 \ldots \mu_n$ dieses Ideals $\mathfrak{m}$, während alles Uebrige unverändert bleibt; mithin ist $\Delta(\Omega)$ durch

$$\Delta(\mu_1, \mu_2 \ldots \mu_n) = N(\mathfrak{m})^2 \Delta(\Omega)$$

zu ersetzen, und der Grenzwerth dieser auf alle Ideale $\mathfrak{e}$ bezüglichen Summe ist $= g : N(\mathfrak{m})$.

Durchläuft nun $\mathfrak{a}$ alle Ideale einer beliebigen Classe A, so giebt es ein Ideal $\mathfrak{m}$ der Art, dass alle Producte $\mathfrak{am}$ Ideale der Hauptclasse E werden, und da umgekehrt, wenn $\mathfrak{e}$ ein durch $\mathfrak{m}$ theilbares Ideal $\mathfrak{am}$ der Hauptclasse E ist, $\mathfrak{a}$ gewiss der Classe A angehört, so ist

$$\Sigma \frac{s-1}{N(\mathfrak{a})^s} = N(\mathfrak{m})^s \Sigma \frac{s-1}{N(\mathfrak{e})^s},$$

und folglich

$$\lim \Sigma \frac{s-1}{N(\mathfrak{a})^s} = g,$$

d. h. jede auf eine bestimmte Idealclasse bezügliche Partialsumme nähert sich demselben Grenzwerthe g. Bezeichnet man daher mit $h(\Omega)$ die *Anzahl* aller dieser Idealclassen, so ist der Grenzwerth der Totalsumme gleich $gh(\Omega)$, und folglich ist

$$h(\Omega) = \frac{r i^{\nu-n} \sqrt{\Delta(\Omega)}}{2^{\nu-1} \pi^{n-\nu} L} \lim \Sigma \frac{(s-1)\tau(m)}{m^s}$$

oder halb so gross, wenn $n = 2\nu$ ist. Die Bestimmung der Classenanzahl ist hiermit auf die von der Theorie der Ideale zu leistende Bestimmung der Function $\tau(m)$ zurückgeführt*).

---

*) Für die aus der Kreistheilung entspringenden Körper führt dieselbe, wie *Kummer* gezeigt hat, zu den Reihen, welche in dem Dirichlet'schen Beweise des Satzes über die arithmetische Progression (Supplement VI) auftreten; vergl. die Anm. zu §. 163, 3.

§. 168.

Wir wollen nun zum Schlusse die vorhergehenden allgemeinen Untersuchungen auf die quadratischen Körper anwenden, um von dem gewonnenen Standpunct aus den Hauptgegenstand dieses Werkes noch einmal zu überblicken.

Ist die ganze rationale Zahl D keine Quadratzahl und auch durch kein Quadrat (ausser 1) theilbar, so bilden die Zahlen $t+u\sqrt{D}$, wenn t, u alle rationalen Zahlen durchlaufen, einen quadratischen Körper, welcher durch die beiden Substitutionen $\varphi(t+u\sqrt{D}) = t \pm u\sqrt{D}$ in sich selbst übergeht. Setzt man $\theta = \frac{1}{2}(1+\sqrt{D})$ oder $= \sqrt{D}$, je nachdem $D \equiv 1 \pmod 4$ ist oder nicht, so bilden die Zahlen $1, \theta$ eine Grundreihe des Körpers, und seine Grundzahl Δ ist entsprechend $= D$ oder $= 4D$. Die quadratische Gleichung, welcher θ genügt, sei

$$f(\theta) = \theta^2 - b\theta + c = 0,$$

so ist $x + y\theta$ mit $x + y(b-\theta)$ conjugirt, und

$$\Delta = (2\theta - b)^2 = b^2 - 4c.$$

Ist nun $\mathfrak{p}$ irgend ein Primideal des Körpers, und p die durch $\mathfrak{p}$ theilbare positive rationale Primzahl, so ist $N(\mathfrak{p}) = p^2$ oder $= p$, je nachdem $\mathfrak{i}(p) = \mathfrak{p}$ oder ein Product aus zwei Primidealen $\mathfrak{p}, \mathfrak{p}'$ ist. Im letzteren Falle bilden die Zahlen $0, 1, 2 \ldots (p-1)$, weil sie incongruent sind, ein vollständiges Restsystem (mod. $\mathfrak{p}$), d. h. jede ganze Zahl des Körpers ist einer rationalen ganzen Zahl congruent; mithin giebt es auch eine rationale ganze Zahl t, welcher θ congruent ist, und folglich ist $f(t) = t^2 - bt + c$ eine ganze rationale durch $\mathfrak{p}$, also auch durch p theilbare Zahl, d. h.

$$t^2 - bt + c \equiv 0 \pmod p,$$

oder in der Sprache der Theorie der höheren Congruenzen: die quadratische Function $f(x) = x^2 - bx + c$ ist nach dem Modul p congruent einem Producte aus zwei Functionen ersten Grades $(x-t)$ und $(x-b+t)$ mit rationalen Coefficienten. Umgekehrt: hat die Congruenz $f(x) \equiv 0 \pmod p$ eine rationale Wurzel $x \equiv t$, so ist

$$f(t) = (t-\theta)(t-b+\theta) \equiv 0 \pmod p;$$

wäre nun $\mathfrak{i}(p)$ ein Primideal, so müsste wenigstens einer der Factoren $(t-\theta)$, $(t-b+\theta)$ durch p theilbar sein, was aber nicht der Fall ist, weil die Zahlen 1, θ eine *Grundreihe* des Körpers bilden; mithin ist $\mathfrak{i}(p) = \mathfrak{p}\mathfrak{p}'$ ein Product aus zwei Primidealen $\mathfrak{p}$ und $\mathfrak{p}'$, deren Normen $= p$ sind; ist nun $t-\theta$ durch $\mathfrak{p}$ theilbar, also $\mathfrak{i}(t-\theta) = \mathfrak{p}\mathfrak{q}$, so ist $\mathfrak{q}$ nicht theilbar durch $\mathfrak{p}'$, weil sonst $(t-\theta)$ durch p theilbar wäre, und da $\mathfrak{i}(t-\theta)\,\mathfrak{i}(t-b+\theta) = \mathfrak{p}\mathfrak{q}\,\mathfrak{i}(t-b+\theta)$ durch $\mathfrak{i}(p) = \mathfrak{p}\mathfrak{p}'$ theilbar ist, so muss $(t-b+\theta)$ durch $\mathfrak{p}'$ theilbar sein; man kann daher

$$\theta \equiv t \pmod{\mathfrak{p}}, \quad \theta \equiv b-t \pmod{\mathfrak{p}'}$$

setzen, und $\mathfrak{p}$, $\mathfrak{p}'$ *conjugirte* Primideale nennen, weil aus $x+y\theta \equiv 0 \pmod{\mathfrak{p}}$ stets $x+y(b-\theta) \equiv 0 \pmod{\mathfrak{p}'}$ folgt.

Es fragt sich nun, ob diese beiden Primideale $\mathfrak{p}$, $\mathfrak{p}'$ identisch sein können. Dann muss $\theta \equiv t \equiv b-t \pmod{\mathfrak{p}}$, also $2t-b$ durch $\mathfrak{p}$ und folglich auch durch p theilbar sein, und da $4f(t) = (2t-b)^2 - \Delta \equiv 0 \pmod{p}$ ist, so muss

$$\Delta \equiv 0 \pmod{p}$$

sein. Umgekehrt: ist p eine in der Grundzahl $\Delta = b^2-4c$ aufgehende rationale Primzahl, so giebt es immer eine ganze rationale t, welche den beiden Congruenzen

$$f(t) \equiv 0, \quad 2t \equiv b \pmod{p}$$

genügt; ist nämlich p ungerade, so ist t durch die zweite Congruenz bestimmt, und aus $4f(t) = (2t-b)^2 - \Delta$ folgt $f(t) \equiv 0$; ist aber $p = 2$, also b gerade, so ist t durch die erste Congruenz $f(t) \equiv t^2 + c \equiv 0 \pmod{2}$ bestimmt, nämlich $t \equiv c \pmod{2}$, und die zweite Congruenz ist ebenfalls erfüllt. Aus der Existenz einer rationalen Wurzel t der Congruenz $f(t) \equiv 0$ folgt aber, wie oben gezeigt ist, $\mathfrak{i}(p) = \mathfrak{p}\mathfrak{p}'$, wo $\mathfrak{p}$ und $\mathfrak{p}'$ zwei Primideale bedeuten, für welche $\theta \equiv t \pmod{\mathfrak{p}}$, $\theta \equiv b-t \pmod{\mathfrak{p}'}$ ist; da nun ausserdem $t \equiv b-t \pmod{p}$ ist, so folgt, dass $(\theta - t)$ sowohl durch $\mathfrak{p}$ als auch durch $\mathfrak{p}'$ theilbar ist; wären nun $\mathfrak{p}$ und $\mathfrak{p}'$ verschieden, also relative Primideale, so müsste $(\theta - t)$ auch durch $\mathfrak{p}\mathfrak{p}'$, d. h. durch p theilbar sein; da dies nicht der Fall ist, so sind $\mathfrak{p}$ und $\mathfrak{p}'$ identisch, also ist $\mathfrak{i}(p) = \mathfrak{p}^2$. Wir sind mithin zu folgendem Resultat gelangt:

Geht die rationale Primzahl p in der Grundzahl Δ auf, so ist $\mathfrak{i}(p) = \mathfrak{p}^2$ das Quadrat eines Primideals $\mathfrak{p}$; ist p eine in Δ nicht aufgehende Primzahl, so ist $\mathfrak{i}(p) = \mathfrak{p}\mathfrak{p}'$ ein Product aus zwei

verschiedenen Primidealen $\mathfrak{p}, \mathfrak{p}'$, *oder* $\mathfrak{i}(p)$ *ein Primideal, je nachdem die Congruenz* $f(t) \equiv 0 \pmod{p}$ *eine rationale Wurzel* t *besitzt oder nicht.*

Die Zahl $p = 2$ bietet den ersten Fall dar, wenn $\Delta \equiv 0 \pmod 4$, also $D \equiv 2, 3 \pmod 4$ ist; ist dagegen $\Delta = D \equiv 1 \pmod 4$, so tritt der zweite oder dritte Fall ein, je nachdem c gerade oder ungerade, d. h. je nachdem $D \equiv 1$ oder $\equiv 5 \pmod 8$ ist. Hieraus erklärt sich das eigenthümliche Verhalten der Zahl 2 in der Theorie der quadratischen Reste (§. 36).

Ist p eine ungerade, in Δ nicht aufgehende rationale Primzahl, so folgt aus $4f(t) = (2t - b)^2 - \Delta$, dass der zweite oder dritte Fall eintritt, je nachdem

$$\left(\frac{\Delta}{p}\right) = \left(\frac{D}{p}\right) = +1 \quad \text{oder} = -1$$

ist. Um alle Fälle am bequemsten zusammenzufassen, führen wir für jede positive ganze rationale Zahl m eine Charakteristik (Δ, m) der Art ein, dass

$$(\Delta, mm') = (\Delta, m)\,(\Delta, m')$$

und, wenn p eine rationale Primzahl bedeutet,

$$(\Delta, p) = 0, \quad = +1, \quad = -1$$

ist, je nachdem $\mathfrak{i}(p)$ Quadrat eines Primideals, oder ein Product aus zwei verschiedenen Primidealen, oder selbst ein Primideal ist. Bedeutet nun $\tau(m)$ die Anzahl aller verschiedenen Ideale $\mathfrak{a}$, deren Normen $= m$ sind, so ist

$$\tau(p^r) = (\Delta, 1) + (\Delta, p) + (\Delta, p^2) + \cdots + (\Delta, p^r),$$

und allgemein

$$\tau(m) = \Sigma\,(\Delta, n),$$

wo n alle Divisoren von m durchläuft. Hieraus folgt (vergl. §§. 89, 91, 124)

$$\Sigma \frac{\tau(m)}{m^s} = \Sigma \frac{1}{m^s} \Sigma \frac{(\Delta, m)}{m^s},$$

also, wenn $(s-1)$ positiv unendlich klein wird,

$$\lim \Sigma \frac{s-1}{N(\mathfrak{a})^s} = \lim \Sigma \frac{(\Delta, m)}{m^s},$$

wo m nur alle diejenigen positiven ganzen rationalen Zahlen zu durchlaufen braucht, welche relative Primzahlen zu Δ sind, oder auch

$$\lim \Sigma \frac{s-1}{N(\mathfrak{a})^s} = \frac{1}{1-\frac{(\Delta, 2)}{2}} \cdot \lim \Sigma \left(\frac{D}{n}\right) \frac{1}{n^s},$$

wo n alle relativen Primzahlen zu $2D$ durchläuft. Substituirt man dies in den allgemeinen Ausdruck des vorigen Paragraphen für die Anzahl der Idealclassen, so findet man, dass dieselbe vollständig übereinstimmt mit der Classenanzahl der (positiven) ursprünglichen Formen der Determinante D, und zwar der zweiten Art, wenn $D \equiv 1 \pmod 4$ ist; der Grund für diese Uebereinstimmung liegt, wie man leicht erkennt, darin, dass jede Formenclasse nur einer einzigen Idealclasse entspricht (vergl. §. 165, 2.).

§. 169.

Sind α, β zwei von einander unabhängige ganze Zahlen eines quadratischen Körpers Ω, und durchlaufen die Variabeln x, y alle ganzen rationalen Zahlen, so bilden die Zahlen

$$\mu = x\alpha + y\beta \tag{1}$$

einen aus lauter ganzen Zahlen bestehenden Modul $\mathfrak{m}$ (§. 161); umgekehrt, wenn ein Modul $\mathfrak{m}$ aus ganzen Zahlen μ des Körpers Ω besteht und zwei von einander unabhängige Zahlen enthält, so sind alle Zahlen μ von der Form (1), wo α, β zwei particuläre Zahlen des Moduls bedeuten; bilden die Zahlen ω_1, ω_2 eine bestimmte Grundreihe des Körpers Ω, so kann man die Basiszahlen

$$\alpha = p_1\omega_1 + p_2\omega_2, \quad \beta = q_1\omega_1 + q_2\omega_2$$

immer so wählen, dass $(p_1q_2 - q_1p_2)$ positiv ausfällt, und dann mag α die erste, β die zweite Basiszahl des Moduls $\mathfrak{m}$ heissen. Nun wird

$$N(\mu) = m(ax^2 + bxy + cy^2), \tag{2}$$

wo m den Theiler der quadratischen Form $N(\mu)$, also eine positive ganze rationale Zahl bedeutet, während a, b, c ganze rationale Zahlen ohne gemeinschaftlichen Theiler sind. Setzt man

$$b^2 - 4ac = d, \tag{3}$$

und bezeichnet mit α_1, β_1 die resp. mit α, β conjugirten Zahlen, so ist

$$\alpha\alpha_1 = ma, \quad \alpha\beta_1 + \beta\alpha_1 = mb, \quad \beta\beta_1 = mc,$$

folglich die Discriminante

$$\Delta(\alpha, \beta) = dm^2. \tag{4}$$

Wählt man statt α, β irgend eine andere Basis desselben Moduls $\mathfrak{m}$, so leuchtet ein, dass die Zahlen m und d unverändert bleiben, und dass die entsprechenden ursprünglichen Formen $ax^2+bxy+cy^2$ eine Formenclasse bilden; die Zahlen m und d können füglich die *Norm* und *Determinante des Moduls* $\mathfrak{m}$ genannt werden. Ersetzt man die Variabeln x und y resp. durch β und $-\alpha$, so ergiebt sich

$$a\beta^2 - b\alpha\beta + c\alpha^2 = 0, \quad b\beta - 2c\alpha = \beta\sqrt{d}. \tag{5}$$

Ist ausserdem

$$g = h\alpha + k\beta$$

die kleinste positive ganze rationale Zahl des Moduls $\mathfrak{m}$, so sind h, k relative Primzahlen, und wenn man

$$ah^2 + bhk + ck^2 = e$$

setzt, so ergiebt sich $N(g) = g^2 = me$; mithin ist e positiv und geht in g^2 auf. Da α, β ganze Zahlen sind, so findet man ferner leicht, dass dg^2 durch e^2 theilbar sein muss; bedeutet daher f^2 das grösste in d und e aufgehende Quadrat, so muss fg durch e theilbar sein. Soll ferner $\mathfrak{m}$ ein Ideal im weiteren Sinne des Wortes sein (§. 165, 4.), sollen also α^2, $\alpha\beta$, β^2 ebenfalls in $\mathfrak{m}$ enthalten sein, so muss g durch e theilbar sein; doch werden wir im Folgenden von dieser Voraussetzung absehen.

Suchen wir nun die *Ordnung* $\mathfrak{n}$ des Moduls $\mathfrak{m}$, d. h. das System aller Zahlen ν von der Art, dass jedes Product $\mu\nu$ in $\mathfrak{m}$ enthalten ist (§. 165, 4.), so ist erforderlich und hinreichend, dass

$$\alpha\nu = x\alpha + y\beta, \quad \beta\nu = x'\alpha + y'\beta$$

wird, wo x, y, x', y' ganze rationale Zahlen bedeuten; hieraus folgt durch Elimination von ν

$$y\beta^2 - (y'-x)\alpha\beta - x'\alpha^2 = 0,$$

und hieraus durch Vergleichung mit (5)

$$y = az, \quad y'-x = bz, \quad -x' = cz,$$

wo z eine ganze rationale Zahl sein muss, weil a, b, c keinen gemeinschaftlichen Theiler haben. Mithin wird

$$\nu = x + \frac{a\beta}{\alpha} z,$$

wo x und z willkürliche ganze rationale Zahlen bedeuten. Da aus (5)

$$N(\nu) = x^2 + bxz + acz^2$$

folgt, so sind die Norm und Determinante von $\mathfrak{n}$ resp. $= 1$ und d.

Bezeichnet man ganz allgemein die Anzahl der in einem Modul $\mathfrak{b}$ enthaltenen Zahlen, welche in Bezug auf einen Modul $\mathfrak{a}$ incongruent sind, mit $(\mathfrak{b}, \mathfrak{a})$, so ergiebt sich aus

$$g = h\alpha + k\beta$$

$$g\frac{\alpha\beta}{\omega} = -ck\alpha + (ah + bk)\beta$$

nach leicht zu beweisenden allgemeinen Sätzen*)

$$(\mathfrak{n}, \mathfrak{m}) = \frac{g^2}{u}, \quad (\mathfrak{m}, \mathfrak{n}) = \frac{e}{u}, \quad (\mathfrak{n}, \mathfrak{m}) = m(\mathfrak{m}, \mathfrak{n}),$$

wo u den grössten gemeinschaftlichen Divisor von g und e bedeutet. Ist $\mathfrak{m}$ ein Ideal, also ein Vielfaches von $\mathfrak{n}$, so ist $(\mathfrak{m}, \mathfrak{n}) = 1$, $(\mathfrak{n}, \mathfrak{m}) = m$.

§. 170.

Sind $\mathfrak{m}$, $\mathfrak{m}'$ zwei Moduln von der eben betrachteten Beschaffenheit, deren Zahlen μ, μ' demselben quadratischen Körper Ω angehören, so bilden alle Producte $\mu\mu'$ und deren Summen wieder einen solchen Modul $\mathfrak{m}'' = \mathfrak{m}\mathfrak{m}'$. Uebertragen wir die vorhergehenden Bezeichnungen durch Accentuation von $\mathfrak{m}$ auf $\mathfrak{m}'$ und $\mathfrak{m}''$, so müssen *erstens*, weil alle Producte $\mu\mu'$ in $\mathfrak{m}''$ enthalten sind, acht ganze rationale Zahlen $p, q \ldots p''', q'''$ existiren, welche den Gleichungen

$$\begin{aligned} \alpha\alpha' &= p\alpha'' + q\beta'' \\ \alpha\beta' &= p'\alpha'' + q'\beta'' \\ \beta\alpha' &= p''\alpha'' + q''\beta'' \\ \beta\beta' &= p'''\alpha'' + q'''\beta'' \end{aligned} \tag{1}$$

*) Vergl. §. 161. Anm. — Ich erwähne hier nur noch Folgendes. Nennt man zwei Moduln $\mathfrak{a}$, $\mathfrak{b}$ verwandt, wenn $(\mathfrak{a}, \mathfrak{b})$ und $(\mathfrak{b}, \mathfrak{a})$ endlich sind, so sind zwei mit $\mathfrak{a}$ verwandte Moduln $\mathfrak{b}$, $\mathfrak{c}$ auch mit einander verwandt, und es ist

$$(\mathfrak{a}, \mathfrak{b})\,(\mathfrak{b}, \mathfrak{c})\,(\mathfrak{c}, \mathfrak{a}) = (\mathfrak{b}, \mathfrak{a})\,(\mathfrak{c}, \mathfrak{b})\,(\mathfrak{a}, \mathfrak{c}),$$

wovon man sich leicht durch die Betrachtung der kleinsten gemeinschaftlichen Vielfachen und grössten gemeinschaftlichen Theiler überzeugt.

genügen. Setzen wir zur Abkürzung*) die aus ihnen gebildeten partialen Determinanten

$$\begin{gathered} pq'-qp'=P,\quad pq''-qp''=Q,\quad pq'''-qp'''=R,\\ p''q'''-q''p'''=U,\quad p'q'''-q'p'''=T,\quad p'q''-q'p''=S, \end{gathered} \tag{2}$$

so ist

$$RS=QT-PU, \tag{3}$$

und durch Elimination von α'', β'' aus je drei der Gleichungen (1) erhält man

$$\begin{aligned} &*\quad U\alpha\beta'-T\beta\alpha'+S\beta\beta'=0\\ -\,&U\alpha\alpha'\quad *\quad +R\beta\alpha'-Q\beta\beta'=0\\ &T\alpha\alpha'-R\alpha\beta'\quad *\quad +P\beta\beta'=0\\ -\,&S\alpha\alpha'+Q\alpha\beta'-P\beta\alpha'\quad *\quad =0. \end{aligned} \tag{4}$$

Eliminirt man T aus der ersten und dritten, ferner U aus der ersten und zweiten dieser Gleichungen, so erhält man

$$\begin{gathered} P\beta^2-(R-S)\alpha\beta+U\alpha^2=0,\\ Q\beta'^2-(R+S)\alpha'\beta'+T\alpha'^2=0, \end{gathered}$$

und folglich muss (zufolge (5) in §. 169)

$$\begin{gathered} P=an',\quad R-S=bn',\quad U=cn',\\ Q=a'n,\quad R+S=b'n,\quad T=c'n \end{gathered} \tag{5}$$

sein, wo n, n' ganze rationale, von Null verschiedene Zahlen bedeuten (denn n' muss eine ganze Zahl sein, weil a, b, c keinen gemeinschaftlichen Theiler haben, und wäre $n'=0$, also auch $P=0$, so wären α', β' zufolge (1) nicht unabhängig von einander); hierdurch nimmt die erste der Gleichungen (4) die Form

$$(b\beta-2c\alpha)\beta'n'=(b'\beta'-2c'\alpha')\beta n$$

an, mithin ist (zufolge (5) in §. 169)

$$n'\sqrt{d}=n\sqrt{d'}, \tag{6}$$

und hiermit sind die vier Gleichungen (4) vollständig befriedigt. Das Product dd' ist, wie zu erwarten war, eine Quadratzahl.

Da *zweitens* alle Zahlen μ'' des Moduls $\mathfrak{m}''$ durch Addition von Producten $\mu\mu'$ entstehen, so existiren acht ganze rationale Zahlen $u, v \ldots u''', v'''$, welche den Bedingungen

*) Die Bezeichnungen schliessen sich an die an, welche *Gauss* in den artt. 235, 236 der *Disquisitiones Arithmeticae* gewählt hat; die nothwendigen Modificationen sind leicht zu erkennen.

$$\begin{aligned} \alpha'' &= u\alpha\alpha' + u'\alpha\beta' + u''\beta\alpha' + u'''\beta\beta' \\ \beta'' &= v\alpha\alpha' + v'\alpha\beta' + v''\beta\alpha' + v'''\beta\beta' \end{aligned} \tag{7}$$

genügen. Substituirt man hierin die Gleichungen (1), und berücksichtigt, dass die Zahlen α'', β'' von einander unabhängig sind, so folgt

$$\begin{aligned} pu + p'u' + p''u'' + p'''u''' &= 1 \\ qu + q'u' + q''u'' + q'''u''' &= 0 \end{aligned} \tag{8}$$

und

$$\begin{aligned} pv + p'v' + p''v'' + p'''v''' &= 0 \\ qv + q'v' + q''v'' + q'''v''' &= 1. \end{aligned} \tag{9}$$

Bildet man die Determinante aus diesen vier Summen, so erhält man eine Gleichung von der Form

$$PP_1 + QQ_1 + RR_1 + SS_1 + TT_1 + UU_1 = 1, \tag{10}$$

wo die Determinanten $P_1 \ldots U_1$ auf dieselbe Weise aus den Zahlen $u, v \ldots u''', v'''$ gebildet sind, wie $P \ldots U$ aus $p, q \ldots p''', q'''$, und hieraus folgt, dass die sechs Zahlen (2) keinen gemeinschaftlichen Theiler haben. Dasselbe Resultat erhält man auch auf folgendem Wege; eliminirt man jede der vier Zahlen u, u', u'', u''' aus den beiden Gleichungen (8), so folgt

$$\begin{aligned} q &= \ * \ - Pu' - Qu'' - Ru''' \\ q' &= Pu \ * \ - Su'' - Tu''' \\ q'' &= Qu + Su' \ * \ - Uu''' \\ q''' &= Ru + Tu' + Uu'' \ * \end{aligned} \tag{11}$$

ebenso erhält man aus (9) die Gleichungen

$$\begin{aligned} p &= \ * \ Pv' + Qv'' + Rv''' \\ p' &= -Pv \ * \ + Sv'' + Tv''' \\ p'' &= -Qv - Sv' \ * \ + Uv''' \\ p''' &= -Rv - Tv' - Uv'' \ * \end{aligned} \tag{12}$$

Aus (11) folgt, dass jeder gemeinschaftliche Theiler der sechs Determinanten (2) in den vier Zahlen q, q', q'', q''', mithin zufolge (9) auch in der Zahl 1 aufgeht, was zu beweisen war. Hieraus ergiebt sich leicht mit Rücksicht auf (3), dass auch die sechs Zahlen (5) keinen gemeinschaftlichen Theiler haben; geht nämlich e in P, Q, $R - S$, $R + S$, T, U auf, so sind die Zahlen $2R$, $2S$ ebenfalls theilbar durch e, und die Quotienten $2R:e$ und $2S:e$ sind ent-

weder beide gerade oder beide ungerade, weil ihre Summe gerade ist; wären sie nun beide ungerade, so wäre auch ihr Product $4RS:e^2$ ungerade, was gegen die Gleichung (3) streitet, der zufolge RS durch e^2 theilbar ist; mithin sind R und S durch e theilbar, und folglich ist $e = \pm 1$. Es ergiebt sich daher, dass n und n' *relative Primzahlen* sind.

Durch Elimination der vier Zahlen α, β, α', β' aus den Gleichungen (1) erhält man

$$(p'\alpha'' + q'\beta'')\,(p''\alpha'' + q''\beta'') = (p\alpha'' + q\beta'')\,(p'''\alpha'' + q'''\beta'')$$

oder

$$L\beta''^2 - M\alpha''\beta'' + N\alpha''^2 = 0, \tag{13}$$

wenn man zur Abkürzung

$$\begin{gathered} q'q'' - qq''' = L, \quad p'p'' - pp''' = N, \\ pq''' + qp''' - p'q'' - q'p'' = M \end{gathered} \tag{14}$$

setzt. Wir zeigen zunächst, dass diese drei Zahlen durch nn' theilbar sind; da nämlich zufolge (5)

$$Q \equiv 0, \quad S \equiv -R, \quad T \equiv 0 \pmod{n}$$

ist, so ergiebt sich aus (11) und (12) in Bezug auf denselben Modul

$$\begin{aligned} q &\equiv -Pu' - Ru''', & p &\equiv Pv' + Rv''' \\ q' &\equiv Pu + Ru'', & p' &\equiv -Pv - Rv'' \\ q'' &\equiv -Ru' - Uu''', & p'' &\equiv Rv' + Uv''' \\ q''' &\equiv Ru + Uu'', & p''' &\equiv -Rv - Uv'' \end{aligned}$$

und hieraus

$$L \equiv (PU - R^2)\,(u'u'' - uu'''), \quad N \equiv (PU - R^2)\,(v'v'' - vv'''),$$
$$M \equiv (PU - R^2)\,(u'v'' + v'u'' - uv''' - vu'''),$$

nun ist aber zufolge (3) $PU \equiv R^2 \pmod{n}$, folglich sind L, M, N theilbar durch n; da ferner auf dieselbe Weise sich zeigen lässt, dass sie auch durch n' theilbar sind, so müssen sie, weil n, n' relative Primzahlen sind, auch durch nn' theilbar sein; was zu beweisen war.

Führt man endlich die unabhängigen Variabeln x, y, x', y' und die bilinearen Functionen

$$\begin{aligned} x'' &= pxx' + p'xy' + p''yx' + p'''yy' \\ y'' &= qxx' + q'xy' + q''yx' + q'''yy' \end{aligned} \tag{15}$$

ein, so ergiebt sich durch Elimination von xx', xy', yx', yy'

$$\begin{aligned} py'' - qx'' &= \quad * \quad Pxy' + Qyx' + Ryy' \\ p'y'' - q'x'' &= -Pxx' \; * \; + Syx' + Tyy' \\ p''y'' - q''x'' &= -Qxx' - Sxy' \; * \; + Uyy' \\ p'''y'' - q'''x'' &= -Rxx' - Txy' - Uyx' \; * \end{aligned}$$

und hieraus folgt

$$\begin{aligned} &(p'y'' - q'x'')\,(p''y'' - q''x'') - (py'' - qx'')\,(p'''y'' - q'''x'') \\ &= (Px^2 + (R - S)\,xy + Uy^2)\,(Qx'^2 + (R + S)\,x'y' + Ty'^2), \end{aligned} \tag{16}$$

d. h.

$$\begin{aligned} &Lx''^2 + Mx''y'' + Ny''^2 \\ &= nn'(ax^2 + bxy + cy^2)\,(a'x'^2 + b'x'y' + c'y'^2). \end{aligned} \tag{17}$$

Da diese Gleichung eine Identität in Bezug auf die Variabeln x, y, x', y' wird, sobald x'', y'' durch die Ausdrücke (15) ersetzt werden, so muss, wenn enn' den grössten gemeinschaftlichen Divisor von L, M, N bedeutet, e in allen neun Producten aa', ab' ... cc' aufgehen; diese letzteren haben aber keinen gemeinschaftlichen Theiler, weil dasselbe sowohl von den Zahlen a, b, c, wie von den Zahlen a', b', c' gilt; mithin ist $e = 1$, also nn' *der grösste gemeinschaftliche Theiler von* L, M, N. Nun ist ferner in Folge der bilinearen Substitution (15)

$$x''\alpha'' + y''\beta'' = (x\alpha + y\beta)\,(x'\alpha' + y'\beta'),$$

folglich auch

$$N(x''\alpha'' + y''\beta'') = N(x\alpha + y\beta)\,N(x'\alpha' + y'\beta'),$$

also

$$\begin{aligned} &m''(a''x''^2 + b''x''y'' + c''y''^2) = \\ &mm'(ax^2 + bxy + cy^2)\,(a'x'^2 + b'x'y' + c'y'^2); \end{aligned}$$

mithin ergiebt sich durch Vergleichung mit (17)

$$nn'm''\,(a''x''^2 + b''x''y'' + c''y''^2) = mm'(Lx''^2 + Mx''y'' + Ny''^2);$$

diese Gleichung, welche eine Identität in Bezug auf die Variabeln x, y, x', y' wird, sobald x'', y'' durch die Ausdrücke (15) ersetzt werden, muss deshalb auch eine Identität in Bezug auf x'', y'' sein; da ferner m, m', m'' positiv sind, und die Zahlen a'', b'', c'' keinen gemeinschaftlichen Theiler haben, so ergiebt sich

$$n'' = mm' \tag{18}$$

und

$$L = a''nn', \quad M = b''nn', \quad N = c''nn', \tag{19}$$

also

$$\begin{aligned} &a''x''^2 + b''x''y'' + c''y''^2 \\ &= (ax^2 + bxy + cy^2)\ (a'x'^2 + b'x'y' + c'y'^2). \end{aligned} \tag{20}$$

Da endlich aus der Definition der Grössen (2) und (14), oder auch aus (16) sich leicht ergiebt, dass

$$\begin{aligned} &M^2 - 4LN \\ &= (R-S)^2 - 4PU = (R+S)^2 - 4QT \end{aligned}$$

ist, so folgt hieraus schliesslich

$$d''n^2n'^2 = dn'^2 = d'n^2,$$

d. h. die Determinante d'' ist der grösste gemeinschaftliche Theiler der beiden Determinanten

$$d = d''n^2, \quad d' = d''n'^2, \tag{21}$$

woraus sich leicht ergiebt, dass die Ordnung $\mathfrak{n}''$ des Productmoduls $\mathfrak{m}'' = \mathfrak{m}\mathfrak{m}'$ auch das Product nn' aus den Ordnungen $\mathfrak{n}$, $\mathfrak{n}'$ von $\mathfrak{m}$, $\mathfrak{m}'$ ist. Ist ferner $\mathfrak{m}'$ das System $\mathfrak{o}$ aller ganzen Zahlen des Körpers Ω, so wird $\mathfrak{m}''$ ein Ideal im engeren Sinne des Wortes, nämlich der grösste gemeinschaftliche Theiler der beiden Ideale $\mathfrak{i}(\alpha)$, $\mathfrak{i}(\beta)$ oder aller Ideale $\mathfrak{i}(\mu)$; zugleich ist $m' = 1$, $m'' = m = N(\mathfrak{m}'')$, und $d' = d'' = \Delta(\Omega)$.

Wir stellen uns jetzt noch die Aufgabe, die Zahlen α'', β'' zu finden, wenn die Zahlen a, β, α', β', also auch a, b, c, $\sqrt{d}$, a', b', c', $\sqrt{d'}$ gegeben sind; die nachfolgende Lösung ist, abgesehen von geringfügigen Aenderungen, der eleganten Methode entlehnt, welche von *Gauss* zu ähnlichem Zweck angewandt ist und sich in hohem Grade verallgemeinern lässt (vergl. §. 161, Anm.). Die beiden relativen Primzahlen n, n' sind durch (6), und folglich die sechs ganzen Zahlen $P \ldots U$ durch (5) (bis auf einen gemeinschaftlichen Factor ± 1) aus den Daten vollständig bestimmt, und zwar so, dass sie die Gleichungen (3), (4) befriedigen und keinen gemeinschaftlichen Theiler haben*). Nun wähle man, durch die Gleichungen (11) geleitet, vier ganze rationale Zahlen Ω, Ω', Ω'', Ω''' willkürlich, nur mit der einzigen Beschränkung, dass die folgenden vier Zahlen

*) Dass R und S (zufolge (5)) *ganze* Zahlen werden und keinen gemeinschaftlichen Theiler mit P, Q, T, U haben, geht unmittelbar aus der Gewissheit hervor, dass der Modul $\mathfrak{m}''$ und die Basiszahlen α'', β'' *existiren*; es lässt sich aber auch sehr leicht aus (5) und (6) beweisen, natürlich unter der Voraussetzung, dass dd' eine Quadratzahl ist.

$$\begin{aligned} * \quad P\mathfrak{Q}' + Q\mathfrak{Q}'' + R\mathfrak{Q}''' &= rq \\ -P\mathfrak{Q} \quad * \quad + S\mathfrak{Q}'' + T\mathfrak{Q}''' &= rq' \\ -Q\mathfrak{Q} - S\mathfrak{Q}' \quad * \quad + U\mathfrak{Q}''' &= rq'' \\ -R\mathfrak{Q} - T\mathfrak{Q}' - U\mathfrak{Q}'' \quad * \quad &= rq''' \end{aligned} \tag{22}$$

nicht sämmtlich verschwinden und folglich einen grössten gemeinschaftlichen Divisor r besitzen; nachdem hierdurch vier ganze Zahlen q, q', q'', q''' ohne gemeinschaftlichen Theiler gewonnen sind, wähle man (nach §. 24) vier ganze rationale Zahlen v, v', v'', v''' so, dass

$$qv + q'v' + q''v'' + q'''v''' = 1 \tag{23}$$

wird, und bestimme die Zahlen p, p', p'', p''' durch die Gleichungen (12); endlich wähle man sechs ganze rationale Zahlen P', Q', R', S', T', U' (nach §. 24) so, dass

$$PP' + QQ' + RR' + SS' + TT' + UU' = 1 \tag{24}$$

wird, setze hierauf

$$\begin{aligned} u \quad &= \quad * \quad P'q' + Q'q'' + R'q''' \\ u' &= -P'q \quad * \quad + S'q'' + T'q''' \\ u'' &= -Q'q - S'q' \quad * \quad + U'q''' \\ u''' &= -R'q - T'q' - U'q'' \quad * \end{aligned} \tag{25}$$

und bestimme die Zahlen α'', β'' durch die Gleichungen (7), so bilden dieselben eine Basis des Moduls $\mathfrak{m}''$, d. h. sie genügen den Gleichungen (1).

Um sich hiervon zu überzeugen, bemerke man zunächst, dass aus (22) mit Rücksicht auf (3) die Relationen

$$\begin{aligned} * \quad Uq' - Tq'' + Sq''' &= 0 \\ -Uq \quad * \quad + Rq'' - Qq''' &= 0 \\ Tq - Rq' \quad * \quad + Pq''' &= 0 \\ -Sq + Qq' - Pq'' \quad * \quad &= 0 \end{aligned}$$

folgen; mit Hülfe derselben ergiebt sich aus (12) und (23)

$$\begin{aligned} pq' - qp' &= (Pv' + Qv'' + Rv''')q' - (-Pv + Sv'' + Tv''')q \\ &= P(qv + q'v') + (Qq' - Sq)v'' + (Rq' - Tq)v''' \\ &= P(qv + q'v' + q''v'' + q'''v''') = P, \end{aligned}$$

und auf ähnliche Weise erhält man die fünf anderen Gleichungen (2). Mithin folgt die erste der beiden Gleichungen (8), wenn man die Gleichungen (25) mit p, p', p'', p''' multiplicirt und mit Rück-

sicht auf (24) addirt; die zweite Gleichung (8) ergiebt sich unmittelbar aus (25), wenn man mit q, q', q'', q''' multiplicirt und addirt. Es gelten daher auch die aus (8) und (2) abgeleiteten Gleichungen (11). Von den Gleichungen (9) findet die zweite zufolge (23) Statt, während die erste sich aus (12) ergiebt, wenn man mit v, v', v'', v''' multiplicirt und addirt. Setzt man ferner zur Abkürzung

$$uv' - vu' = P_1, \quad uv'' - vu'' = Q_1, \quad uv''' - vu''' = R_1,$$
$$u'v''' - v''u''' = U_1, \quad u'v''' - v'u''' = T_1, \quad u'v'' - v'u'' = S_1,$$

so ergiebt sich die Gleichung (10) entweder auf die dort angegebene Weise aus (8) und (9), oder auch aus (12), wenn man mit u, u', u'', u''' multiplicirt und unter Rücksicht auf (8) addirt. Substituirt man ferner für p, q ihre Ausdrücke aus (12) und (11), so erhält man

$$\begin{aligned} pu + qv &= PP_1 + QQ_1 + RR_1 \\ pu' + qv' &= QS_1 + RT_1 \\ pu'' + qv'' &= -PS_1 + RU_1 \\ pu''' + qv''' &= -PT_1 - QU_1. \end{aligned}$$

Multiplicirt man diese Gleichungen mit $\alpha\alpha', \alpha\beta', \beta\alpha', \beta\beta'$ und addirt, so folgt aus den Definitionen (7) mit Rücksicht auf (4) und (10) die erste der Gleichungen (1); da die anderen sich auf ganz ähnliche Art ergeben, so bilden die durch die Gleichungen (7) definirten Zahlen α'', β'' in der That eine Basis des Productes $\mathfrak{m}'' = \mathfrak{m}\mathfrak{m}'$, was zu beweisen war.

Wir bemerken zum Schluss, dass man für die ersten Basiszahlen $\alpha, \alpha', \alpha''$ stets die kleinsten positiven ganzen rationalen Zahlen g, g', g'' wählen kann, welche in den Moduln $\mathfrak{m}, \mathfrak{m}', \mathfrak{m}''$ enthalten sind; dann wird $q = 0$, und die Bestimmung von $\mathfrak{m}''$ aus $\mathfrak{m}$ und $\mathfrak{m}'$ lässt sich auf ein System von Congruenzen reduciren, ähnlich wie in dem speciellen Falle, welcher in den §§. 145, 146 behandelt ist*).

*) Vergl. *Arndt: Auflösung einer Aufgabe in der Composition der quadratischen Formen.* Crelle's Journal LVI.

Druckfehler.

Seite 109, Zeile 1 ist zu lesen $\left(\frac{11}{365}\right) = \left(\frac{365}{11}\right) = \left(\frac{2}{11}\right) = -1$.

Seite 157, Zeile 15 ist ψ' statt ψ zu lesen.

Seite 226, Zeile 18 ist *Zahl* statt *Zahlen* zu lesen.